ALTIGEN COMMUNICATIONS
410 East Plumeria Drive • San Jose, CA 95134
www.altigen.com • +1 (408) 597-9000

MaxACD for Lync Release 6.5.8

Deployment Guide

August 2013

Contents

Introduction 3
Operational Notes 3
Requirements 6
Server Requirements 6
MaxAgent Requirements 6
VRM (Voice Recording Manager) Requirements 6
MaxReports Requirements 7
Architecture 8
Installation 9
Step 1: Planning 9
Step 2: Preparation 10
Step 3: Create a New Trusted Application Pool on the Lync Server 11
Step 4: Make the System a Lync Application Server 12
Step 5: Install MaxACD 6.5.8 17
Step 6: Install the UCMA Application Service 20
Step 7: Check the MaxACD System's Firewall Exception List 22
Step 8: Install the Server SDK Proxy on Lync Front-end Servers 23
Step 9: Check Each Lync Front-end Server's Firewall Exception List 25
Step 10: Configure MaxACD to Interact with Lync Server 26
Step 11: Publish the Topology 30
Configuration 32
Step 12: Configure Firewall/NAT Ports 32
Step 13: Configure Exchange Server 33
Step 14: Configure a Lync User as a MaxACD Agent Extension 34
Step 15: Configure Call Routing from Lync Server to MaxACD 36
Step 16: Configure Outbound Workgroup Call Rules 39
Step 17: Configure MaxACD for Lync Routing 41
Step 18: Configure Voicemail Access 44
Troubleshooting 45
Performance 46

AltiGen Communications, Inc.
410 East Plumeria Dr. San Jose, CA 95134
Telephone: 888-AltiGen (258-4436) Fax: 408-597-9020
E-mail: info@altigen.com | Web site: www.altigen.com
Copyright © AltiGen Communications, Inc. 2013. All rights reserved.

Introduction

This guide introduces AltiGen's Call Center product, MaxACD, which handles automatic call distribution. This document details the hardware and software requirements and basic configurations necessary to connect an AltiGen MaxACD to a Microsoft® Lync™ Server.

This guide does not provide instructions for upgrading an existing MaxACD 6.5.7 release to the 6.5.8 release. A separate document, *MaxACD for Lync Release 6.5.8 Upgrade Guide*, provides this information.

AltiGen's MaxACD is an automatic call distribution server for the Microsoft Lync solution. The MaxACD server handles workgroup functions, such as automatic call distribution, workgroup queue management and RTM (Real Time Monitoring) and Supervisor operations. Agents and Supervisors are located in the Microsoft Lync pool, with corresponding MaxACD agent extensions that are set up in a MaxACD server. Microsoft Lync Server proxy joins MaxACD and Microsoft Lync Server to synchronize Lync user states to MaxACD:

- **Offline** – When the user signs out, the MaxACD agent extension becomes a virtual (not registered) extension.
- **Do Not Disturb** – When the user sets DND, the MaxACD agent extension becomes DND.
- **In a Call** – When the user is in a voice call, the agent status of the MaxACD agent extension displays as Busy, for a workgroup call the line state becomes Connected or In Use for a personal call.

MaxACD now allows custom mapping of other Lync states to agent *Ready* or *Not Ready* states.

For seamless integration, the agent can use the Lync 2010 headset or a Lync-certified Polycom USB telephone as the call center telephone. While a Lync-certified SIP phone is usable as a Lync telephone, MaxACD does not support it for workgroup calls.

Workgroup Calls versus Non-workgroup Calls

We do not recommend routing non-workgroup calls through MaxACD.

- Route incoming personal PSTN (public switched telephone network) calls and Lync-to-Lync calls through the Lync Server.
- Route incoming workgroup calls (calls routed to the MaxACD workgroup pilot number from SIP Gateway or Lync Server) through MaxACD.

For agents who will be participating in outbound workgroup calling, route all outbound calls through the MaxACD server.

Operational Notes

- Make sure that all AltiGen approved Lync Server Cumulative update(s) (CUs) have been deployed on your system before you begin. Contact your AltiGen representative or Sales Engineer for this information.
- MaxAgent cannot see (and does not display) calls that do not route through the MaxACD server.
- Personal caller ID is not displayed in MaxSupervisor.

- Supervisors can record*, silently monitor, barge in, or coach two types of calls:
  - » Inbound PSTN workgroup calls.
  - » Outbound PSTN calls made through an agent's extension with an outbound workgroup configured.

  * Supervisors cannot record on demand when "Auto-record to central location" has been enabled for that workgroup.
- Only single-call handing is available for agents. This means that an agent cannot receive a new workgroup call by placing an existing workgroup call on hold. The current call must be completed, transferred, or otherwise handled before the agent will be able to handle a new workgroup call.
- When a workgroup call is transferred out of MaxACD, it becomes a personal call.
- Conference calls are logged as personal calls.
- Statistics are calculated from the active server only. Because of this, after a redundancy switchover occurs, group statistics values will restart from zero.
- In MaxReports, if you want to export the charts in reports 1301 through 1304 and reports 2301 through 2319, generate the reports in PDF format. The Excel reports do not support those charts.
- In MaxAgent, if an agent is already on a call, the agent cannot click the Pickup button to pick up a queued call. This is because only single-call handling is available.
- In a configuration with multiple Lync Front-end servers, if one FE server goes down, calls may intermittently fail. This happens because the Front-end servers are each listed in the DNS, and when calls go through MaxACD, the server will still try to connect to the FE server listed in the DNS table.
- If you change the password for Manager Extension, you will break the connection to MaxReports.
- If an agent's outbound workgroup call status does not appear in MaxAgent, check the URI configuration for that extension:
  - » The extension's URI must match the URI configured in Lync and in Active Directory
  - » The Mediation Service IP must match the FQDN configured in MaxAdministrator
- When an agent's presence is set to Busy, any outbound call will be considered a non-workgroup call. Because of this, extension Caller IDs will not be transmitted; the system trunk number or main number will be used for the call.
- If an agent tries to blind transfer a workgroup call to an invalid trunk number, the agent may not hear an error tone. In addition, the trunk call and the held party may both drop, leaving the agent no indication that the transfer failed. Because of this possibility, we recommend that agents use the supervised transfer method instead of performing blind call transfers.
- If an agent does a supervised transfer using the secondary pop-up window, and the transferred call is routed to a voice messaging number (either directly or indirectly), the transfer may not be handled properly. If this occurs, a message will be displayed indicating that the transfer did not complete. We recommend that agents transfer calls using the primary (first) pop-up window instead of the secondary window.
- Caller ID is not updated when users make supervised federated transfers. In other words, the call will show the Caller ID of the transferring agent, not the Caller ID of the original inbound call.
- Do not change Workgroup call distribution settings during peak call hours. If you do, it may affect system performance.

- If a MaxAgent client fails to auto-update, this can be the result of a redundant environment where the two servers are running different builds of MaxACD.

  To ensure that both the active server and standby server are on the same build, follow this process:

  1. Update the standby server to the new version.
  2. Switch MaxACD control to the standby server.
  3. Update the other server to the new version. If you like, you can switch control back to the original server.
- If you must uninstall the AltiGen Lync Proxy, we recommend that you stop the AltiGen Proxy service beforehand. If you do not stop the service first, you will need to restart the MaxACD server afterwards.
- If your deployment is on Lync Server 2013, and a Lync Front-end server is restarted, MaxAgent will not be able to play workgroup voicemail. This situation occurs, because the AltiGen UCMA Proxy server is no longer connected to that Front-end server. To resolve this issue, restart the AltiGen UCMA Proxy service.
- If you experience issues in a configuration where multiple mediation servers are behind a hardware load balancer, consider adding a registry entry for the mediation IP addresses. This way, MaxACD will read the registry and add those IP addresses to the matching list.

Requirements

This section lists the requirements your system needs in order to run MaxACD; for Lync hardware and software requirements, refer to your Lync documentation.

Server Requirements

Server Hardware Requirements

Note: An Advanced Micro Devices (AMD) CPU does not support the instruction set necessary for HMCP.

- Dedicated Windows Server 2008 or 2008 R2 Standard running on a 64-bit, Quad-core Intel processor @2GHz, 4GB memory, 160GB hard drive.
- Virtual Server – VMware ESX 5.0 or 5.1, or Hyper-V 6.0.6002.18005. Allocate four Intel cores @ 2GHz each, 4GB memory, and 160GB hard drive.

Server Software Requirements

- MaxACD for Lync Release 6.5.8
- Microsoft Lync Server 2010 or 2013
- Microsoft 2010 or 2013 Mediation Server
- Microsoft Exchange 2010 with Unified Messaging (UM) installed (for voice mail integration). Make sure the Exchange and Outlook versions match. For example, you must use Exchange 2010 with Outlook 2010. You must install Microsoft Outlook on the MaxACD system. Only the 32-bit version of Outlook is supported.
- AltiGen Lync Server Proxy 6.5.8 (running on the Front-end Server and on the MaxACD Server)

MaxAgent Requirements

MaxAgent Client Hardware Requirements

- 2GHz CPU
- 1GB available hard drive disk space
- 2GB RAM
- SVGA monitor (1024 x 768) with 256 color display

MaxAgent Client Software Requirements

- MaxAgent for Lync Release 6.5.8
- Lync 2010 or 2013 client
- Windows XP Professional (32-bit only), Vista Business Edition (32-bit or 64-bit), Windows 7 (32-bit or 64-bit), or Windows 8 (32-bit or 64-bit)
- Microsoft .NET 3.5 framework

VRM (Voice Recording Manager) Requirements

- Windows Server 2003, 2008, or 2008 R2
- 2GHz CPU with 2GB RAM
- 100GB available hard drive disk space

MaxReports Requirements

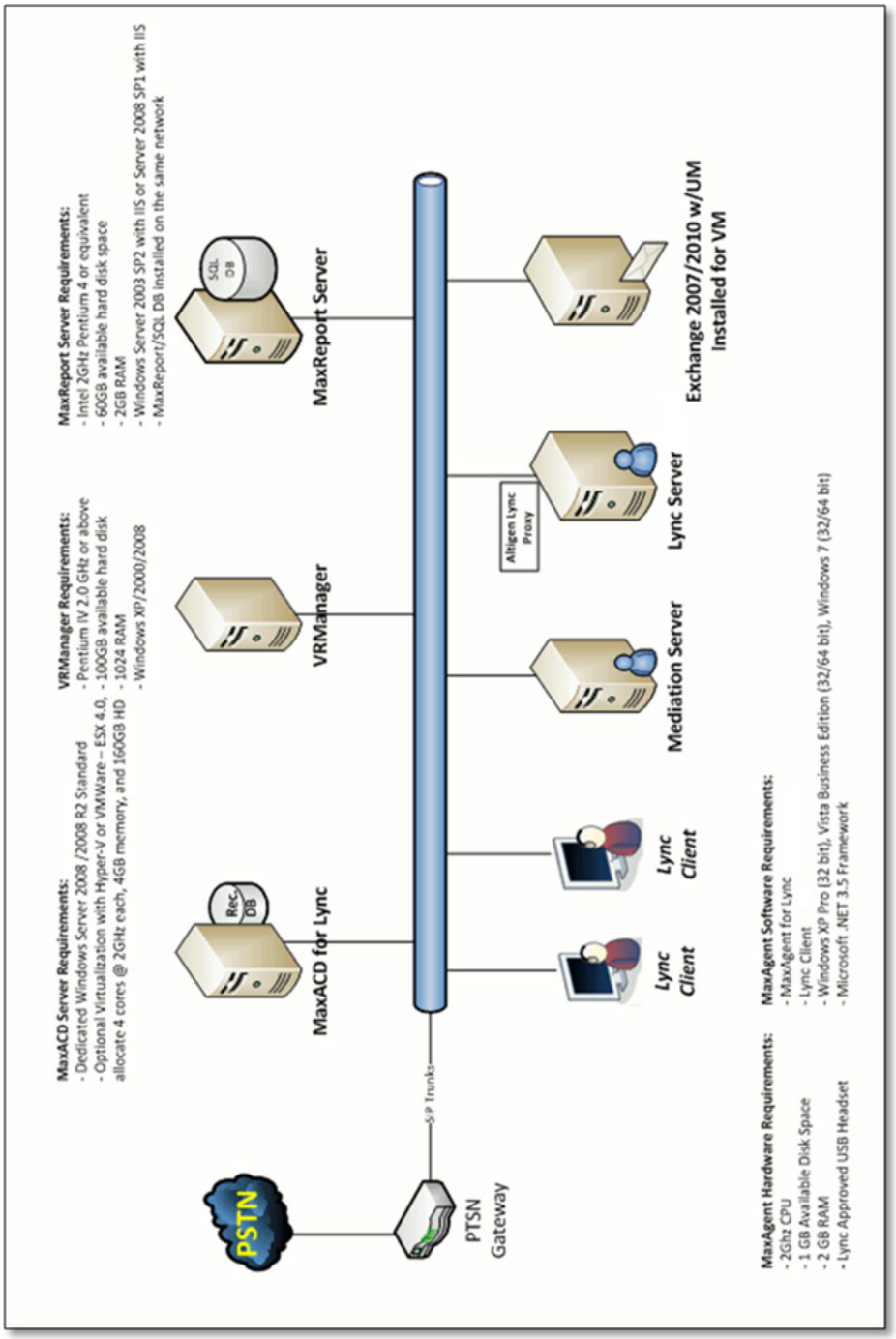
Use a separate server for MaxReports; do not install on the MaxACD system. Minimum system requirements:

- Windows Server 2003, 2008, or 2008 R2
- IBM/PC AT compatible system
- Intel 2GHz Pentium 4 or equivalent CPU
- 100GB available hard drive disk space
- 1GB RAM (2GB RAM are required if run on the same machine as SQL Server. Running MaxReports on the same machine as SQL Server is not recommended.)
- Microsoft Windows Server 2008 SP2 or Microsoft Windows Server 2008 R2
- MaxReports License must be added to MaxACD system and registered.
- JRE 6.0 and Apache Tomcat 6.0; these are included in the MaxReports installation

Additional requirements:

- MaxACD must be installed in the same network
- External Logger and external CDR database (Microsoft SQL Server 2008) must be installed in the same network. External Logger Service must be upgraded to the latest version.
- The client machine must have a suitable Web browser installed (Microsoft Internet Explorer 6.0 or above) prior to installation of MaxReports.

Architecture


MaxACD Server Requirements:
- Dedicated Windows Server 2008 /2008 R2 Standard
- Optional Virtualization with Hyper-V or VMWare – ESX 4.0, allocate 4 cores @ 2GHz each, 4GB memory, and 160GB HD
VRManager Requirements:
- Pentium IV 2.0 GHz or above
- 100GB available hard disk
- 1024 RAM
- Windows XP/2000/2008
MaxReport Server Requirements:
- Intel 2GHz Pentium 4 or equivalent
- 60GB available hard disk space
- 2GB RAM
- Windows Server 2003 SP2 with IIS or Server 2008 SP1 with IIS
- MaxReport/SQL DB installed on the same network
PSTN
PTSN Gateway
SIP Trunks
MaxACD for Lync
Rec. DB
VRManager
MaxReport Server
SQL DB
Lync Client
Lync Client
Mediation Server
Altigen Lync Proxy
Lync Server
Exchange 2007/2010 w/UM Installed for VM
MaxAgent Hardware Requirements:
- 2Ghz CPU
- 1 GB Available Disk Space
- 2 GB RAM
- Lync Approved USB Headset
MaxAgent Software Requirements:
- MaxAgent for Lync
- Lync Client
- Windows XP Pro (32 bit), Vista Business Edition (32/64 bit), Windows 7 (32/64 bit)
- Microsoft .NET 3.5 Framework

Installation

Note: If you are upgrading from MaxACD release 6.5.7, follow the instructions in the *MaxACD for Lync Release 6.5.8 Upgrade Guide* instead of the instructions in this document.

Step 1: Planning

In order to provide optimum connectivity, and to minimize future problems, the following items should be considered prior to attempting to deploy a MaxACD server. Making these decisions prior to configuring MaxACD will streamline the connectivity process.

- **Route Access Digit and IP Trunk Access Digit** – In order to provide outbound workgroup calling through MaxACD, at least one leading digit must be assigned to function as "Route Access". By convention, this is usually the digit '9' (as in "dial 9 to get an outside line); however, MaxACD will support any digit except 0 (zero) for this purpose. It is not possible to create extensions in MaxACD that begin with this "Route Access" digit. In addition to Route Access Digit, an IP Trunk Access Digit needs to be assigned which is usually the digit '8.'
- **Extension Length** – All extensions in the MaxACD server must be of the same length. Typically, this value is set to three or four digits; however, an extension length of up to six digits is supported.

  Caution: Once an extension length is set, the only way to change it is to start with a clean installation and re-program the MaxACD server. For this reason, you should start with a longer extension length if in doubt.
- **Extension Numbers and Workgroup Numbers** – Valid extension numbers in MaxACD can be any set of digits matching the extension length and starting with numbers 1 through 9, as long as the first digit is not assigned to another purpose, such as Route Access or IP trunk access.

  Workgroup numbers can be any number that is valid as an extension number. While there is no requirement that workgroup numbers be sequential, or of any other particular pattern, creating sequential workgroup numbers will simplify creating normalization rules in the Lync dial plan.
- **MaxACD Dial Tone Pilot Number** – Many workgroup features, such as agent login and logout, can be accessed either by using the MaxAgent for Lync client application, or via a dialed feature code. In order to dial the feature code, the agent must first be able to access dial tone on the MaxACD system. The MaxACD dial tone pilot number will allow the agent to do this. This document uses "222" as an example for this number. Following these instructions, a user dialing 222 from Lync will hear dial tone from the MaxACD system. They could then enter a feature code such as #90 (Ready to receive workgroup calls), #54 (agent login), or #56 (agent logout) after hearing this dial tone.

  Configuration of the MaxACD dial tone pilot number is optional, but is recommended. If it is not configured, agents will still be able to use MaxAgent for Lync to control these features.
- **Redundancy Planning** – If you plan to set up a redundant MaxACD system with two different servers, you will do that after you install and configure MaxACD. See the chapter in the *MaxACD Administrator Manual* for full instructions.

Step 2: Preparation

We recommend that you gather the following information before you begin the installation process:

- The Exchange Client Access Server FQDN on which the SSL IMAP4 service is running
- The Exchange Web Service's FQDN
- The SQL Store associated with the Lync Monitoring Server database (this can be retrieved from the Lync Topology builder, by selecting the monitoring pool, and checking for "associations")
- The FQDN of each server that will be running MaxACD Proxy

Plan for various new elements in your Lync environment:

- A new Trusted Application Pool name

Perform the following steps on the server where you want to run MaxACD:

- Install Windows Server 2008 R2, and apply Service Pack 1 (if it is not already installed).
- Join the server to the same domain as your Lync Server.
- If you are installing MaxACD into a Lync 2013 environment:
    - » Install .NET 4.5
    - » Install Windows Management Framework 3.0 (which includes Powershell Script V3.0)
    - » Install Windows Identity Foundation (KB974405)

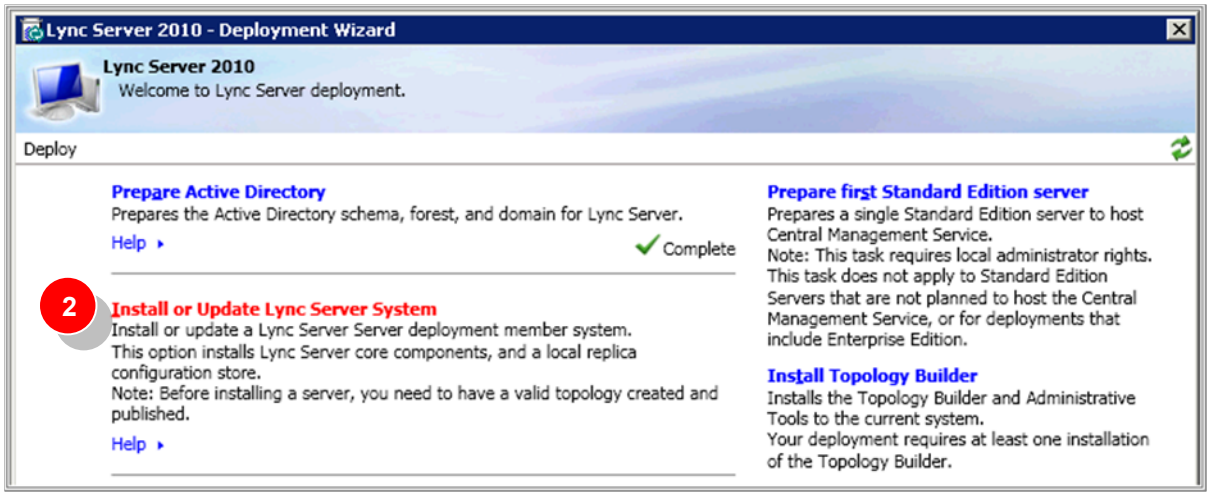
Step 3: Create a New Trusted Application Pool on the Lync Server

1. Log into the Lync Front-end server as a Domain user with Administrative privileges.
2. Open Lync Server and download the topology from your existing deployment.
3. Run **Topology Builder** and create a new Trusted Application pool.
4. Enter a name for this pool. It must be a unique FQDN. This should be different from the FQDN of the server that will be added to the pool. For example, the server FQDN may be *max-proxy.company.com*, and the pool FQDN may be *max-pool.company.com*.
5. Choose **Multiple computer pool**, and then click **Next**.
6. The next page is where you add servers to the pool. You need to enter those servers where MaxACD will be running the Proxy role. Enter each server's FQDN and click **Add**. When you are done, click **Next**.
7. Select which front-end pool to use as the next hop, and then click **Finish**.
8. Publish the revised topology.

Step 4: Make the System a Lync Application Server

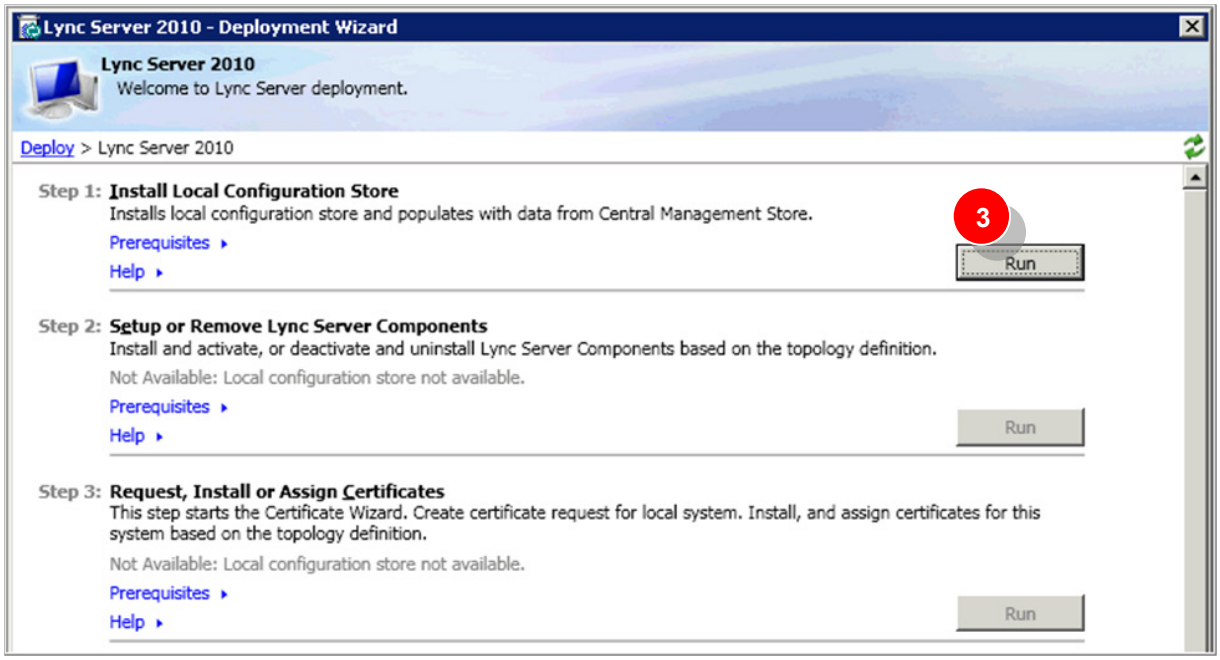
1 On the system where you want to install MaxACD, log in as a Domain user with Administrator privileges. Insert your Lync Server Installation CD and run *setup.exe*.

2 Choose **Install or Update Lync Server System**.

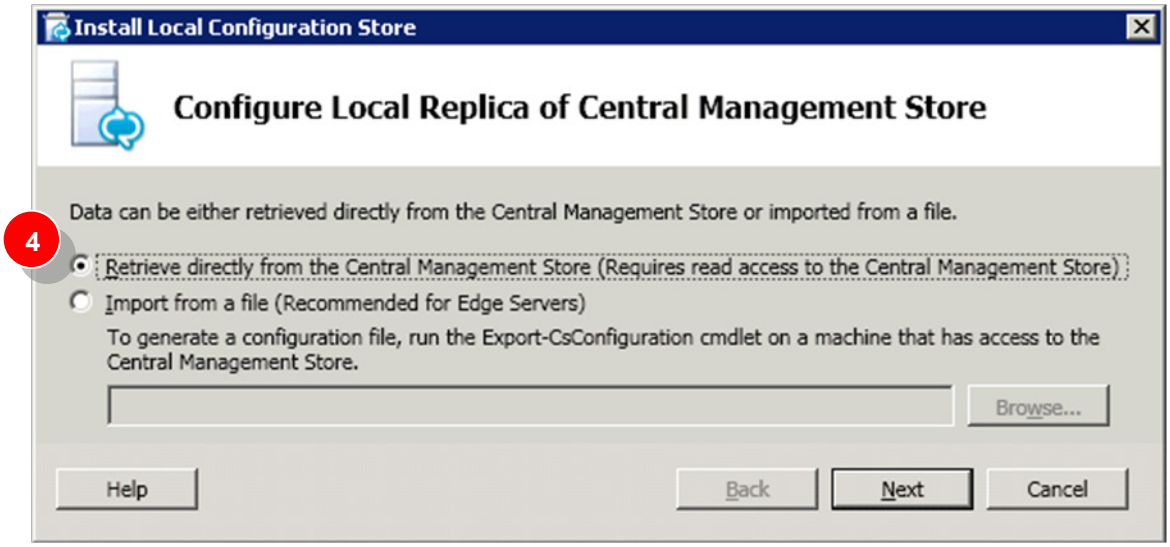

Lync Server 2010 - Deployment Wizard
Lync Server 2010
Welcome to Lync Server deployment.
Deploy
Prepare Active Directory
Prepares the Active Directory schema, forest, and domain for Lync Server.
Help
Complete
2
Install or Update Lync Server System
Install or update a Lync Server Server deployment member system.
This option installs Lync Server core components, and a local replica configuration store.
Note: Before installing a server, you need to have a valid topology created and published.
Help
Prepare first Standard Edition server
Prepares a single Standard Edition server to host Central Management Service.
Note: This task requires local administrator rights. This task does not apply to Standard Edition Servers that are not planned to host the Central Management Service, or for deployments that include Enterprise Edition.
Install Topology Builder
Installs the Topology Builder and Administrative Tools to the current system.
Your deployment requires at least one installation of the Topology Builder.

3 For "Step 1, Install Local Configuration Store," click **Run**.

Note: If you see a warning indicating that a prerequisite step has not been satisfied, you must stop and install 'Windows Identity Foundation,' as noted on page 10.

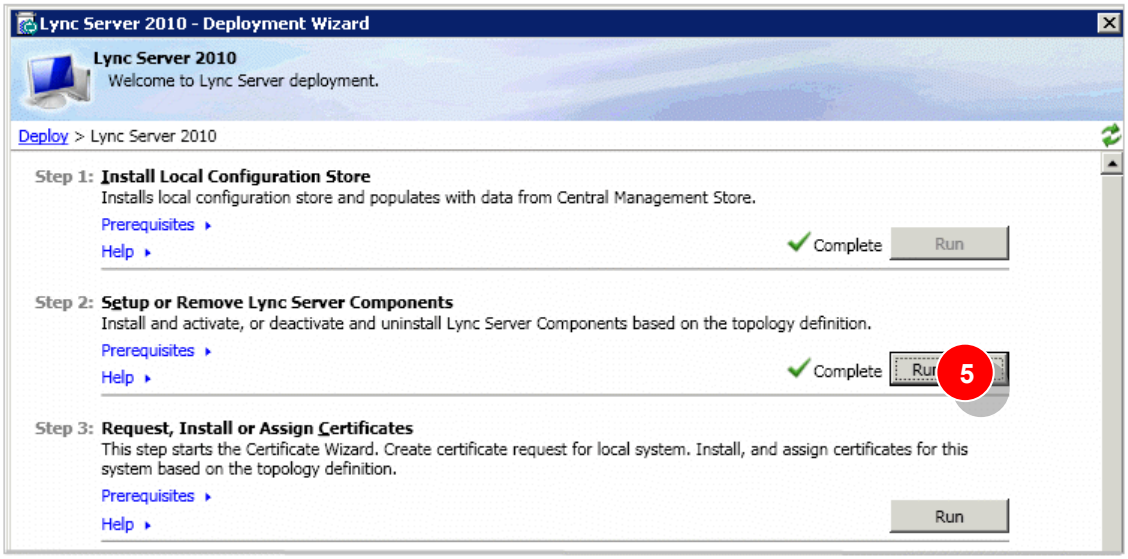

Lync Server 2010 - Deployment Wizard
Lync Server 2010
Welcome to Lync Server deployment.
Deploy > Lync Server 2010
Step 1: Install Local Configuration Store
Installs local configuration store and populates with data from Central Management Store.
Prerequisites
Help
3
Run
Step 2: Setup or Remove Lync Server Components
Install and activate, or deactivate and uninstall Lync Server Components based on the topology definition.
Not Available: Local configuration store not available.
Prerequisites
Help
Run
Step 3: Request, Install or Assign Certificates
This step starts the Certificate Wizard. Create certificate request for local system. Install, and assign certificates for this system based on the topology definition.
Not Available: Local configuration store not available.
Prerequisites
Help
Run

4 On the next pane, choose **Retrieve directly from Central Management Store**, and then click **Next**. When processing has completed, click **Finish**.

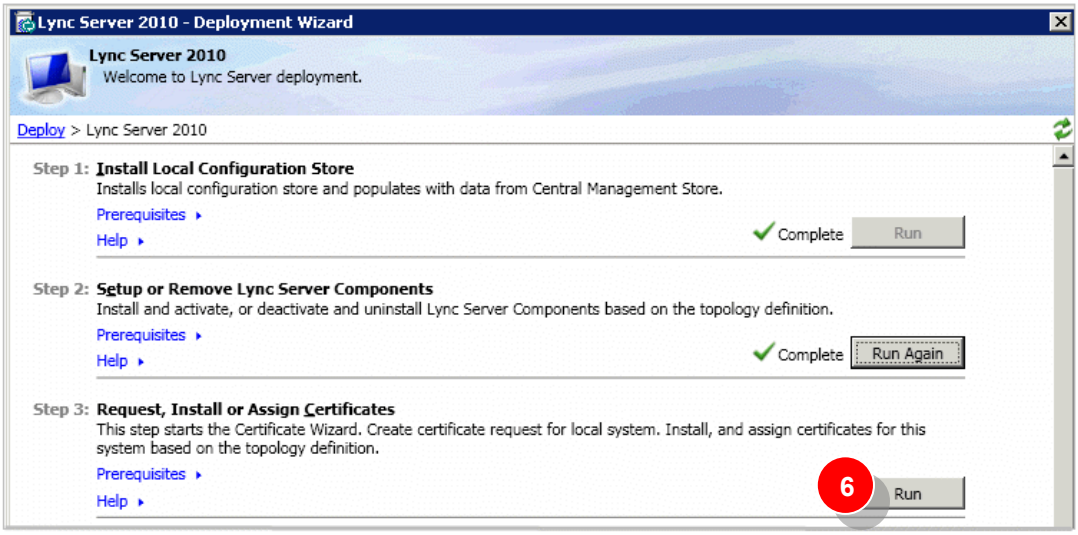

Install Local Configuration Store
Configure Local Replica of Central Management Store
Data can be either retrieved directly from the Central Management Store or imported from a file.
4
Retrieve directly from the Central Management Store (Requires read access to the Central Management Store)
Import from a file (Recommended for Edge Servers)
To generate a configuration file, run the Export-CsConfiguration cmdlet on a machine that has access to the Central Management Store.
Browse...
Help
Back
Next
Cancel

5 You return to the main page. For "Step 2, Setup or Remove Lync Server Components," click **Run** and then click **Next**. When processing has completed, click **Finish**.

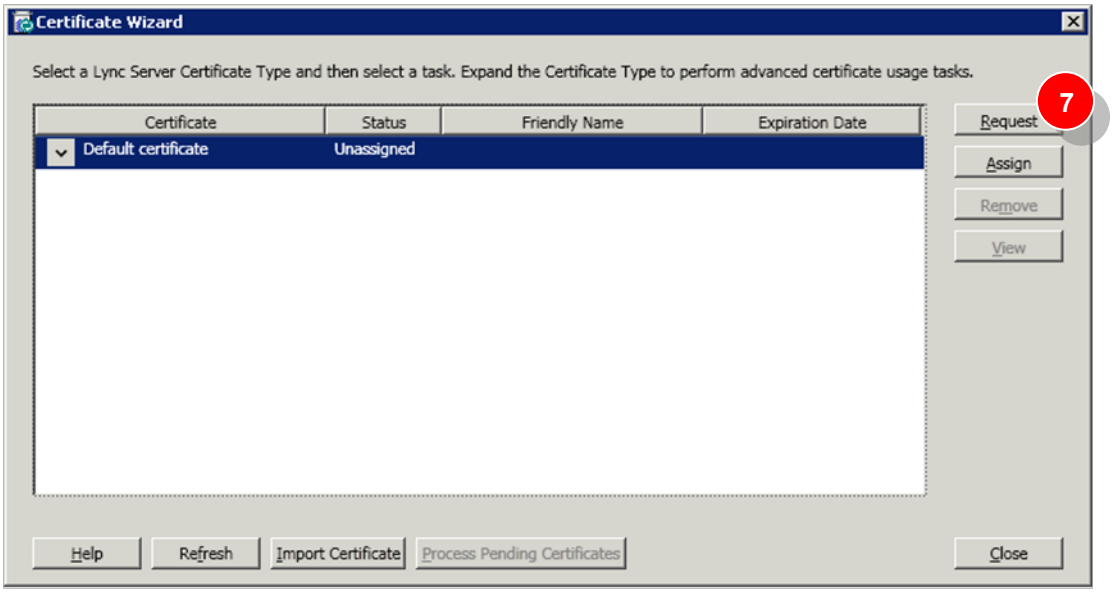
Note: In Lync Server 2013, you may not see the green checkmark when Step 2 is complete.


Lync Server 2010 - Deployment Wizard
Lync Server 2010
Welcome to Lync Server deployment.
Deploy > Lync Server 2010
Step 1: Install Local Configuration Store
Installs local configuration store and populates with data from Central Management Store.
Prerequisites
Help
Complete
Run
Step 2: Setup or Remove Lync Server Components
Install and activate, or deactivate and uninstall Lync Server Components based on the topology definition.
Prerequisites
Help
Complete
Run
5
Step 3: Request, Install or Assign Certificates
This step starts the Certificate Wizard. Create certificate request for local system. Install, and assign certificates for this system based on the topology definition.
Prerequisites
Help
Run

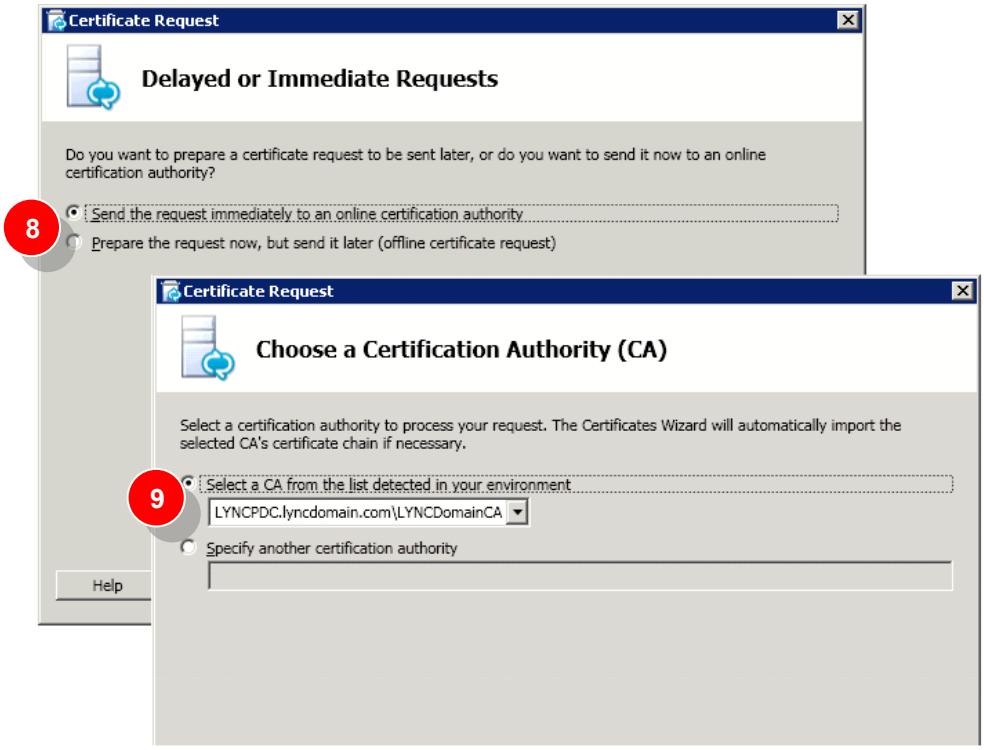
6 When you return to the main page of the Wizard, for "Step 3, Request, Install or Assign Certificates," click **Run**.


Lync Server 2010 - Deployment Wizard
Lync Server 2010
Welcome to Lync Server deployment.
Deploy > Lync Server 2010
Step 1: Install Local Configuration Store
Installs local configuration store and populates with data from Central Management Store.
Prerequisites
Help
Complete
Run
Step 2: Setup or Remove Lync Server Components
Install and activate, or deactivate and uninstall Lync Server Components based on the topology definition.
Prerequisites
Help
Complete
Run Again
Step 3: Request, Install or Assign Certificates
This step starts the Certificate Wizard. Create certificate request for local system. Install, and assign certificates for this system based on the topology definition.
Prerequisites
Help
6
Run

7 In the Certificate Wizard, click **Request**, and then click **Next**.



8 Select the “Send the request immediately…” option and click **Next**.


Certificate Request
Delayed or Immediate Requests
Do you want to prepare a certificate request to be sent later, or do you want to send it now to an online certification authority?
Send the request immediately to an online certification authority
Prepare the request now, but send it later (offline certificate request)
8
Certificate Request
Choose a Certification Authority (CA)
Select a certification authority to process your request. The Certificates Wizard will automatically import the selected CA's certificate chain if necessary.
Select a CA from the list detected in your environment
LYNCPDC.lyncdomain.com\LYNCDomainCA
Specify another certification authority
9
Help

9 Choose the Certificate Authority (CA) from the list and click **Next**.

10 For the next two panels (*Certification Authority Account* and *Specify Alternate Certificate Template*), click **Next** to accept the default settings and continue.

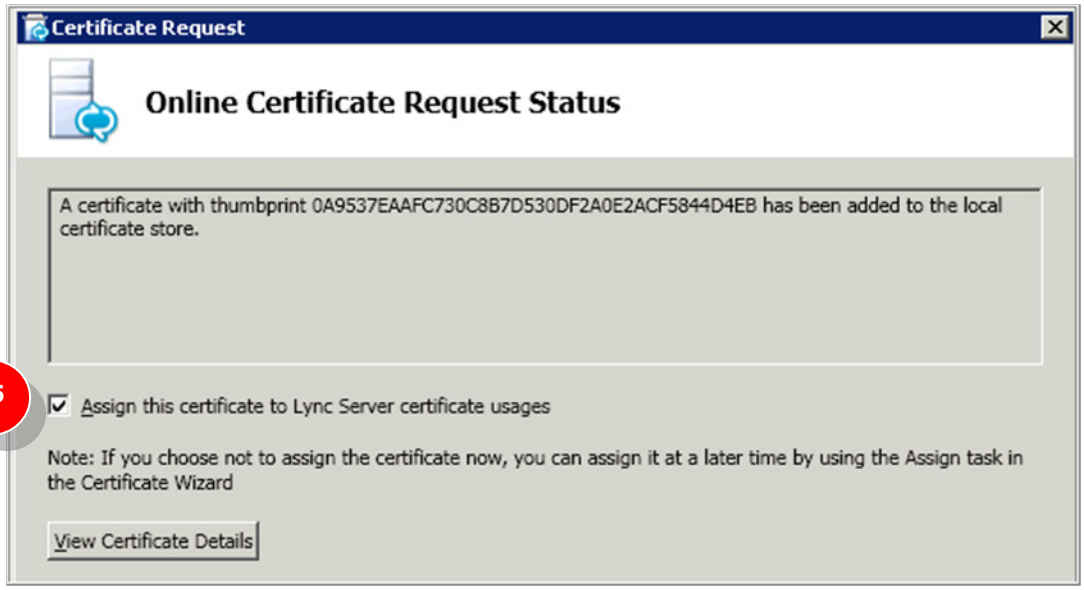
11 When you reach the *Name and Security Settings* panel, enter a friendly name. Make sure that the bit length is set to **2048**, and that the **Mark Certificate Private Key As Exportable** checkbox is checked. Click **Next**.

12 Continue through the wizard panels. When you reach the *Geographical Information* panel, note that names cannot contain abbreviations.

13 Continue through the wizard panels. When you reach the *SIP Domain Setting on Subject Alternate Names* panel, check your SIP domain and click **Next**.

14 Continue through the wizard panels. When you reach the *Certificate Request Summary* panel, review all of the information carefully. If necessary, click **Back** to make any changes. When all of the information is correct, click **Next**. This starts the process of requesting the certificate.

15 When you reach the *Online Certificate Request Status* panel, we recommend that you check the box to assign the certificate (to save yourself a few steps). Click **Finish**, click **Next** twice, and then click **Finish**.


Certificate Request
Online Certificate Request Status
A certificate with thumbprint 0A9537EAAFC730C8B7D530DF2A0E2ACF5844D4EB has been added to the local certificate store.
15
Assign this certificate to Lync Server certificate usages
Note: If you choose not to assign the certificate now, you can assign it at a later time by using the Assign task in the Certificate Wizard
View Certificate Details

16 If you did not check the box in step 11, click **Assign** in the main Certificate pane and assign the certificate.

17 Close the Certificate wizard. When you return to the main page of the Wizard, for "Step 4, Start Services," click **Run**, click **Next,** and click **Finish**.

18 At the bottom of the Deployment window, click **Run** to install any additional Lync updates, and then click **Exit** to close the Deployment wizard.

19 Confirm that the Certificate that you applied to the MaxACD Proxy role is stored in the "Trusted Root Certification Authority" folder on all Lync Front-end servers.

Note: If you split the Mediation and Registrar roles among different servers, make sure that those certificates are also stored in the "Trusted Root Certification Authority" folder on all Lync Front-end servers.

Step 5: Install MaxACD 6.5.8

Follow these steps to install MaxACD.

1 First, obtain a system key and license activation file from your account manager.

2 Log into the system as a Domain or Local user with local administrator privileges, and make sure that the server is already joined to the domain where your Lync Server is installed. If you plan to run Exchange Integration, you must have Domain administrator privileges.

3 Insert the MaxACD CD into the drive of the server. In the **MaxACD Server** > **MaxACD for Lync** folder, run *setup.exe*.

4 Accept the license agreement, and continue to follow the instructions in the wizard.

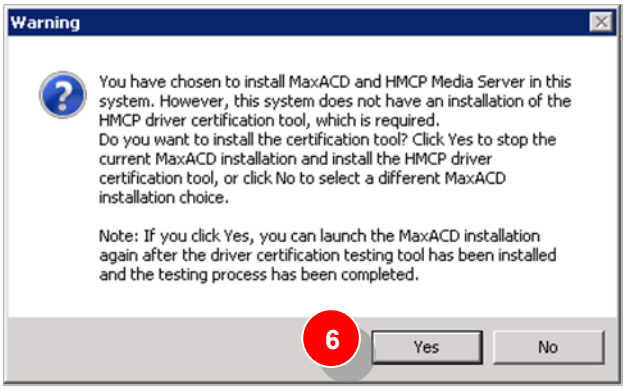
5 When prompted, select a setup type:

- **All-in-one (MaxACD + HMCP) System** – Select this if MaxACD will be operating on a single server. (This is a common configuration.)
- **MaxACD Server with Separate HMCP Server** – Select this if the MaxACD server and HMCP servers will be running on different chassis in an enterprise deployment. You will select which components to install:
  - » **MaxACD Server** – Select this option to install MaxACD on the server. You will need a dongle for the MaxACD server.
  - » **HMCP Media Server** – If you have a small- to medium-size call center (no more than about 200 agents), you can install MaxACD and HMCP Media Server in the same machine. You can also install them in different machines, especially if you plan to grow your call centers.

If you have more than 200 agents, we recommend that you install the HMCP Media Server and MaxACD on two different servers.

6 Before installing the HMCP Media server, the installation program scans the system to determine whether the HMCP Certification Tool has already been installed on that system.

During an All-in-one installation, if the tool is not detected, you must either select **Yes** to install the Certification Tool and automatically restart the MaxACD installation, or select **No** to return to step 5 and select the other installation choice.


Warning
You have chosen to install MaxACD and HMCP Media Server in this system. However, this system does not have an installation of the HMCP driver certification tool, which is required.
Do you want to install the certification tool? Click Yes to stop the current MaxACD installation and install the HMCP driver certification tool, or click No to select a different MaxACD installation choice.
Note: If you click Yes, you can launch the MaxACD installation again after the driver certification testing tool has been installed and the testing process has been completed.
6
Yes
No

7 Continue through the remaining installation panels, entering information as prompted. During this process, the wizard will create a password account for AltiGen services. We recommend that you accept this default password.

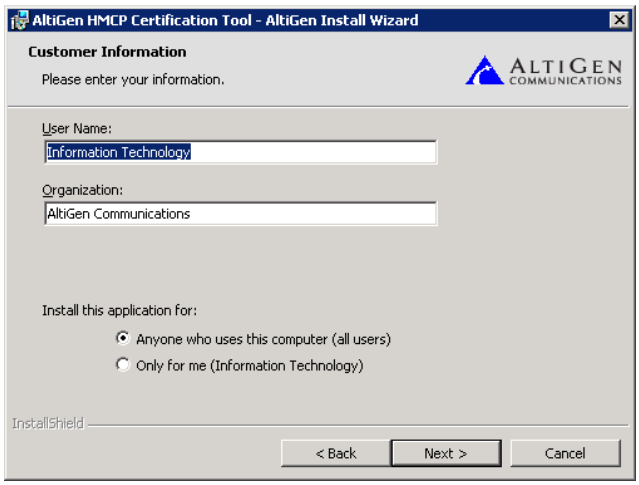
Note: If a window prompts whether to install KEYLOK during the installation process, click **Install**.

8 After the installation process has been completed, you must reboot that system

HMCP Certification Tool Installation

During installation, if you are prompted to install the HMCP certification tool, follow these steps:

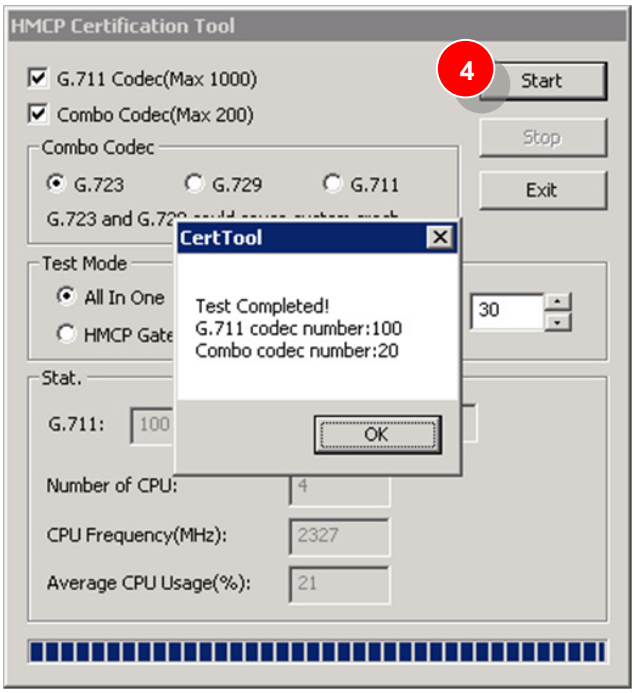
1 Click **Next** through the HMCP tool installation panels, entering information as prompted.



2 On the final panel, click **Finish**. Then click **Yes** to restart the system.

3 After the system restarts, in Windows select **Start** > **All Programs** > **AltiGen HMCP Certification Tool** > **AltiGen HMCP Certification Tool**.

4 In the tool, click **Start**. After the assessment, the tool shows the results. For future configuration, write down the recommended quantities for G711 and combo codecs. Click **OK**, and then click **Exit**.



5 You can now restart the MaxACD installation. Return to *Step 5: Install MaxACD 6.5.8* on page 17 and begin the installation process again.

Step 6: Install the UCMA Application Service on the MaxACD System

The next step is to run the AltiGen Lync Server Proxy installation program to install the UCMA Application Service on the system where you installed MaxACD.

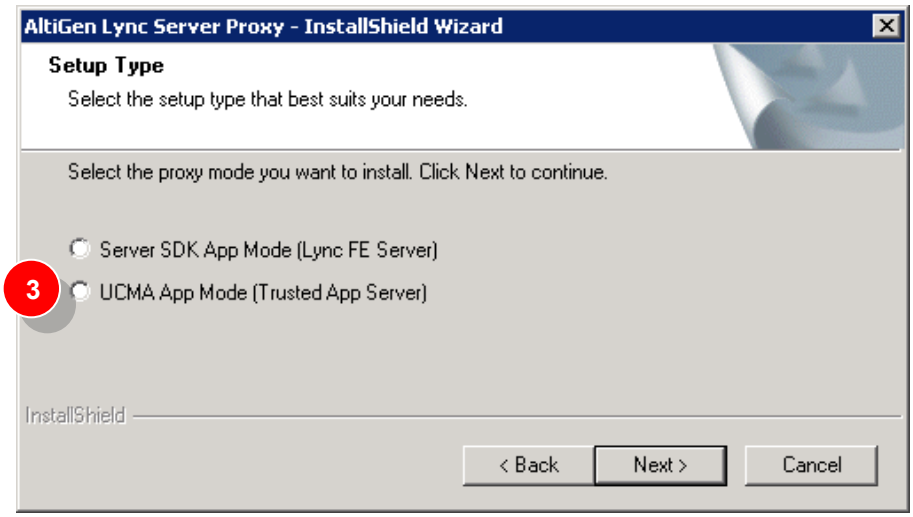
Note: The UCMA Application Proxy can be installed on a different server than the MaxACD server.

The only system that must be added to the Lync Trusted Application Pool and must have Lync deployed to it is the system that is running the UCMA Application Proxy. Therefore, if the UCMA Application Proxy will be installed on a different server than the MaxACD server, then the MaxACD server does not need to be added to the Lync Trusted Application Pool.

1 Log into the system as a Domain user with local Administrator privileges.

2 Insert the MaxACD Installation CD, and in the **MaxACD Server** > **AltiGen Lync Proxy** folder, run *setup.exe*.

3 When prompted, choose **UCMA App Mode (Trusted App Server)** and click **Next**.


AltiGen Lync Server Proxy - InstallShield Wizard
Setup Type
Select the setup type that best suits your needs.
Select the proxy mode you want to install. Click Next to continue.
Server SDK App Mode (Lync FE Server)
3
UCMA App Mode (Trusted App Server)
InstallShield
< Back
Next >
Cancel

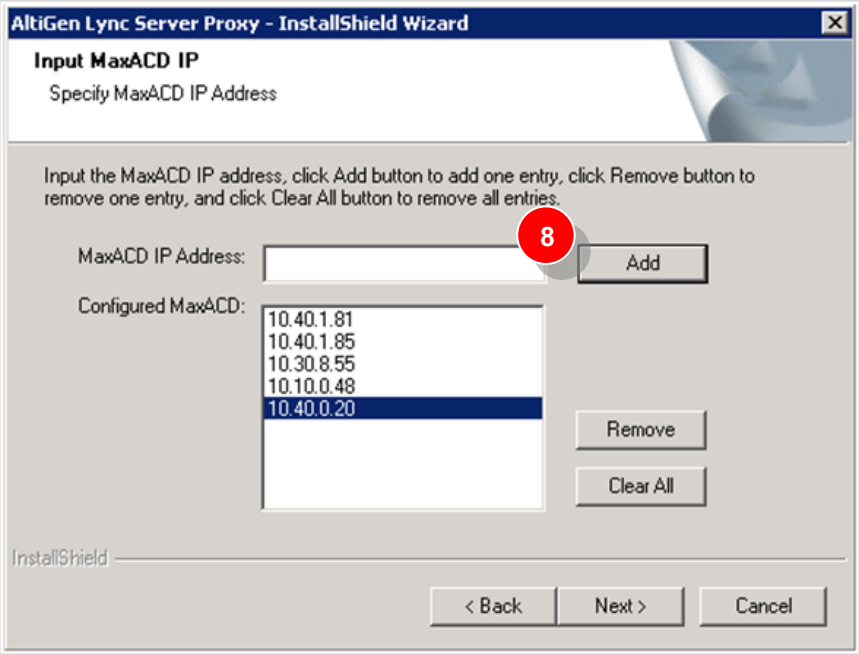
4 Choose which version of Lync is running in your environment, and then click **Next**.

5 When prompted, enter your user name and company name and click **Next**.

6 The setup wizard creates a user account and suggests a random password. If you choose not to use this password, enter a different one (up to 20 characters). Click **Next**.

7 We recommend that you accept the default installation location. Click **Next**.

8 Enter the MaxACD server IP address and click **Add**. To connect to multiple MaxACD servers, enter the IP address of each server. Click **Next** when you are done.



9 Enter the FQDN of the Trusted Application Pool. Click **Next**.

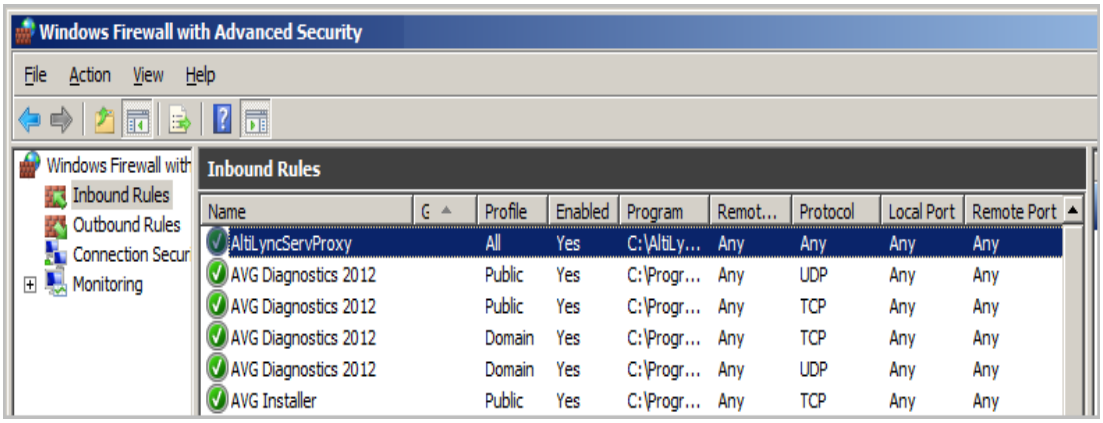
10 Click **Install**. After the process has finished, click **Finish**.

Note: If you need to change the IP addresses in the future, log in as a user with Administrative privileges and run this wizard again. To do this, in Windows, click **Start** > **All Programs**, then right-click *AltiGen Lync Server Proxy Configuration* and select **Run as Admin**.

Step 7: Check the MaxACD System's Firewall Exception List

The installation program is designed to update the list of firewall exceptions on the MaxACD system. You should confirm this list. The steps may vary from one version of Windows to another.

1. On the server where you installed MaxACD, open Windows Firewall (found in the Windows Control Panel, in **System and Security**).
2. Click **Advanced Settings**.
3. Select **Inbound Rules**.
4. Check that the MaxACD system Components list has inbound routing rules established. If not, manually add a new rule.


Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with
Inbound Rules
Outbound Rules
Connection Secur
Monitoring
Inbound Rules
Name | G | Profile | Enabled | Program | Remot... | Protocol | Local Port | Remote Port
AltiLyncServProxy | All | Yes | C:\AltiLy... | Any | Any | Any | Any
AVG Diagnostics 2012 | Public | Yes | C:\Progr... | Any | UDP | Any | Any
AVG Diagnostics 2012 | Public | Yes | C:\Progr... | Any | TCP | Any | Any
AVG Diagnostics 2012 | Domain | Yes | C:\Progr... | Any | TCP | Any | Any
AVG Diagnostics 2012 | Domain | Yes | C:\Progr... | Any | UDP | Any | Any
AVG Installer | Public | Yes | C:\Progr... | Any | TCP | Any | Any

Step 8: Install the Server SDK Proxy on Each Lync Front-end Server

Note: If you have multiple Lync Front-end servers, then the Server SDK Application Proxy must be installed on each one.

The installation account must be a member of the following groups:

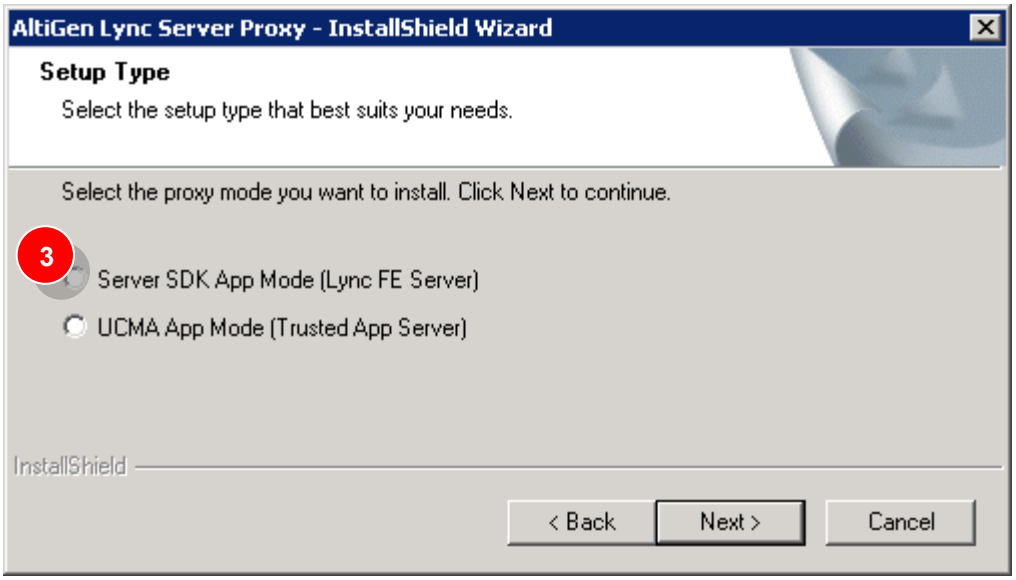
- *RTCUniversalServerAdmins*
- *Account Operator*

In addition, the installation account must be added to *RTC Server Applications* group on the Lync Front-end server.

1 Log in as a Domain user with Administrator privileges.

2 Insert the MaxACD Installation CD, and in the **MaxACD Server** > **AltiGen Lync Proxy** folder, run *setup.exe*.

3 When prompted, choose **Server SDK App Mode (Lync FE Server)** and click **Next**.

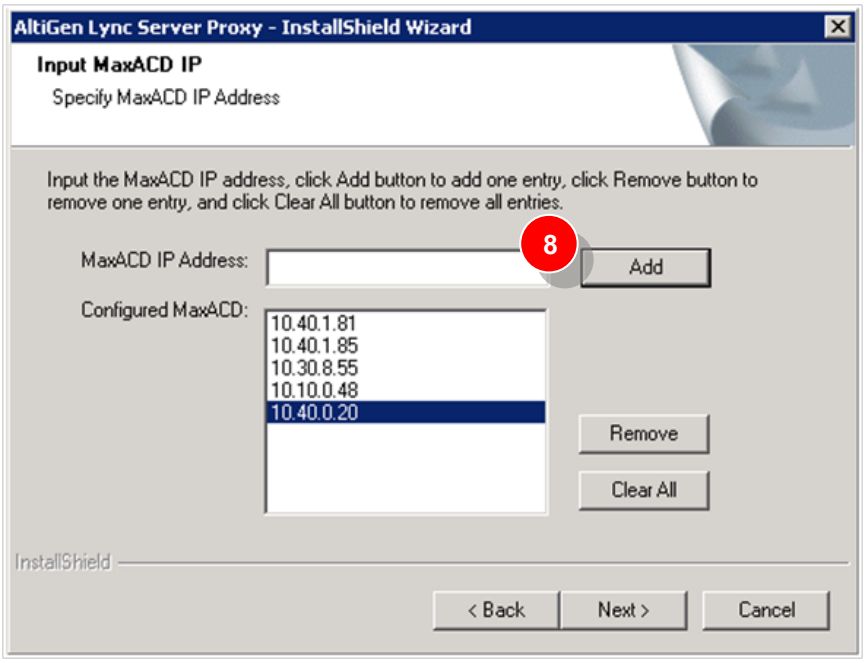

AltiGen Lync Server Proxy - InstallShield Wizard
Setup Type
Select the setup type that best suits your needs.
Select the proxy mode you want to install. Click Next to continue.
3
Server SDK App Mode (Lync FE Server)
UCMA App Mode (Trusted App Server)
InstallShield
< Back
Next >
Cancel

4 Choose which version of Microsoft Lync is running in your environment (2010 or 2013), and then click **Next**.

5 When prompted, enter your user name and company name and click **Next**.

6 The setup wizard creates a user account and suggests a random password. If you choose not to use this password, enter a different one (up to 20 characters). Click **Next**.

7 We recommend that you accept the default installation location. Click **Next**.



8 Enter the MaxACD server IP address and click **Add**. To connect to multiple MaxACD servers, enter the IP address of each server. Click **Next** when you are done.

9 Enter the FQDN of the Lync Front-end Pool. Click **Next**.

Note: You can run `Get-CsSite` from the Lync Server Management Shell on this system to obtain this information.

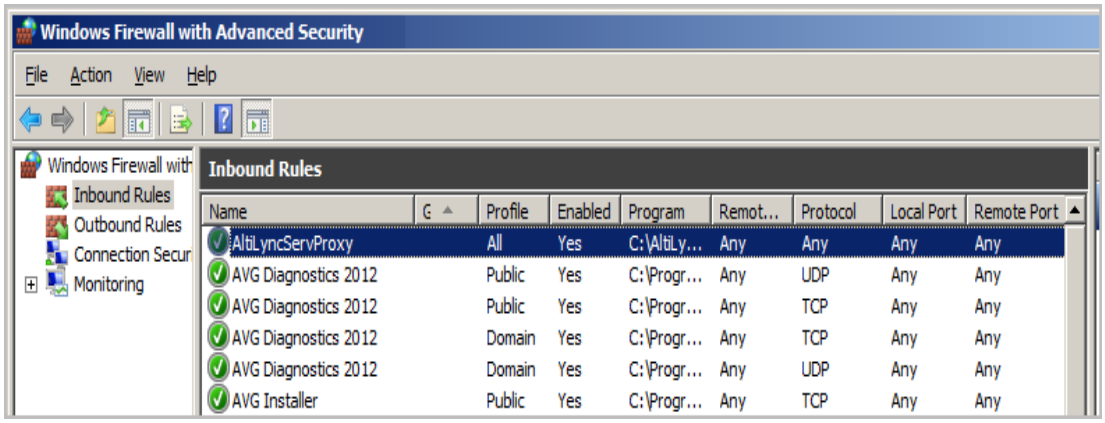
10 Click **Install**. After the process has finished, click **Finish**.

Note: If you need to change the IP addresses in the future, log in as a user with Administrative privileges and run this wizard again. To do this, in Windows, click **Start** > **All Programs**, then right-click *AltiGen Lync Server Proxy Configuration* and select **Run as Admin**.

Step 9: Check Each Lync Front-end Server's Firewall Exception List

The installation program is designed to update the list of firewall exceptions on each Front-end server. You should confirm this list on each server. The steps may vary from one version of Windows to another.

1. On each Lync Front-end server, open Windows Firewall (found in the Windows Control Panel, in **System and Security**).
2. Click **Advanced Settings**.
3. Select **Inbound Rules**.
4. Check that the MaxACD system Components list has inbound routing rules established. If not, manually add a new rule.


Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with
Inbound Rules
Outbound Rules
Connection Secur
Monitoring
Inbound Rules
Name G Profile Enabled Program Remot... Protocol Local Port Remote Port
AltiLyncServProxy All Yes C:\AltiLy... Any Any Any Any
AVG Diagnostics 2012 Public Yes C:\Progr... Any UDP Any Any
AVG Diagnostics 2012 Public Yes C:\Progr... Any TCP Any Any
AVG Diagnostics 2012 Domain Yes C:\Progr... Any TCP Any Any
AVG Diagnostics 2012 Domain Yes C:\Progr... Any UDP Any Any
AVG Installer Public Yes C:\Progr... Any TCP Any Any

Step 10: Configure MaxACD to Interact with Lync Server

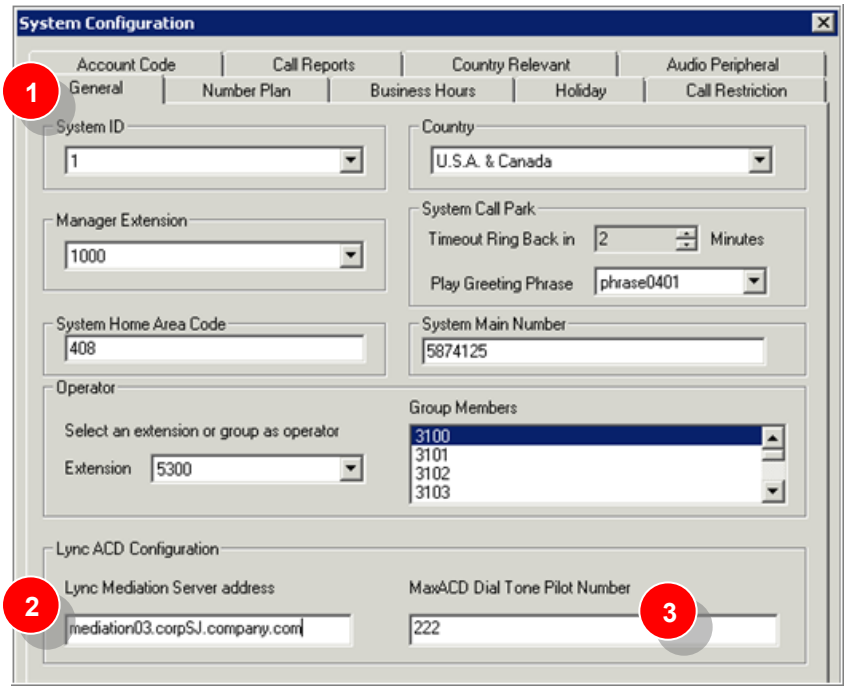
MaxACD accesses the PSTN using SIP trunks by means of the SIP Gateway. DNIS (Dialed Number Identification Service) routing is configured at the SIP Gateway to ensure workgroup calls route to the MaxACD server.

When the SIP Gateway is properly configured, Lync Server and MaxACD can use the same SIP Gateway to gain access to the PSTN.

MaxACD provides multiple levels of AA (Auto Attendant) and data-directed routing capability. We recommend you use the call center AA hosted in MaxACD. Please refer to the *MaxACD Administrator Manual* for detailed configuration.

Configure the Lync Addresses

1 Log into MaxACD Administrator and click **System Configuration** > **General**.



2 Specify the FQDN for the Lync Mediation pool. Do not use an alias. The mediation pool name can be up to 63 characters long.

Note: If you are using a hardware load balancer, you should enter the FQDN of the hardware load balancer instead of the FQDN of the Mediation pool.

3 Enter the MaxACD *Dial Tone Pilot Number*, and click **Apply**.

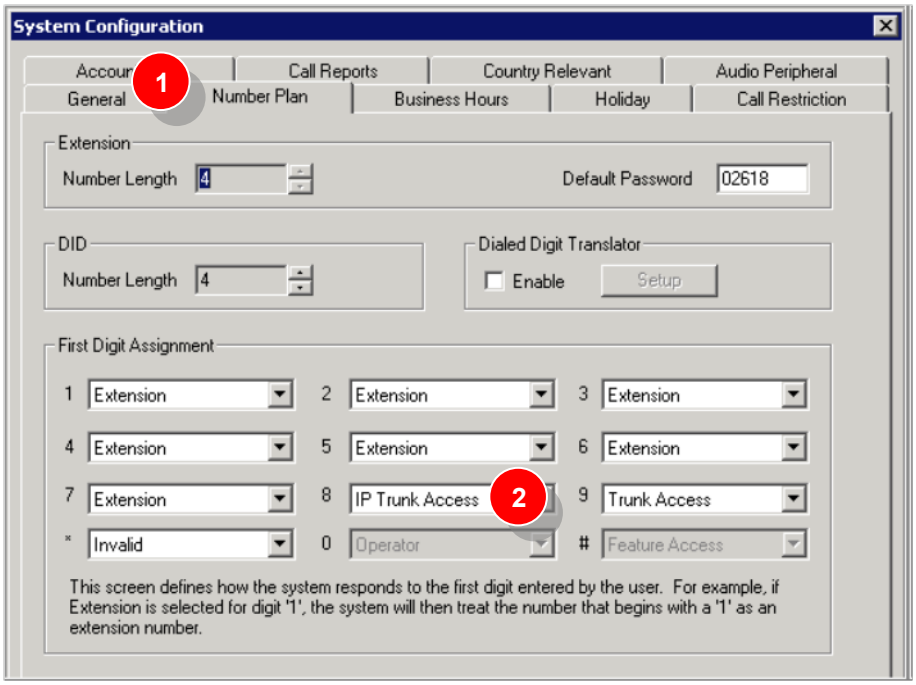
This number is defined in Lync; it allows Lync users to get a MaxACD dial tone. Users can then either dial numbers or press "# #" to access their voicemail mailbox.

Define an IP Trunk Access Digit and apply it to MaxACD SIP-Tie Trunks

In order for calls to successfully route from the MaxACD server to Lync, an IP Trunk Access Digit must be assigned and applied to all SIP-Tie Trunks.

1 Click the *Number Plan* tab.

2 Define a digit as "IP Trunk Access." In the following example, the digit "8" is used.



3 Click **OK**.

4 Next, open the Trunk Configuration page, select any of the SIP-Tie trunks, and set the Trunk Access Code to match the IP Trunk Access digit that was assigned in step 2.

5 Click **Apply To,** leave all of the trunks selected (only SIP-Tie trunks will be present), and click **OK**.

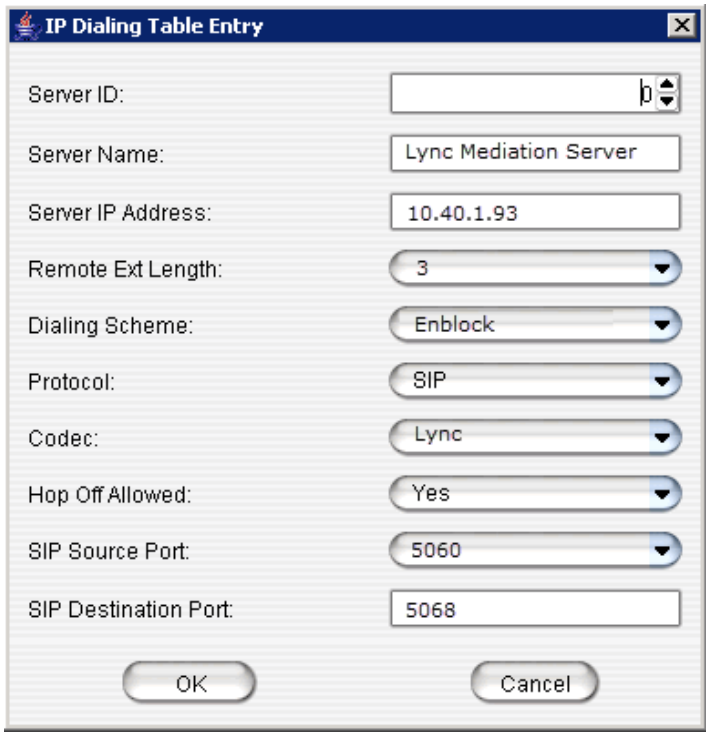
6 In the Trunk configuration window, click **OK** to return to the main MaxACD Administrator window.

Add a New Dialing Table Entry

1 Click **VoIP** > **Enterprise Network Manager** and click the *Server* tab.

2 Click the IP Dialing Table tab and click the Add button below the table.

- Enter a unique server ID (default ID "0" can be used, if available).
- Assign a server name.
- Enter the address of the Lync Mediation Server.
- Set the *Dialing Scheme* to **Enblock**.
- Make the Remote Ext Length the same length as the Lync Server extension length, to avoid a dialing delay.



- Set *Hop Off Allowed* to **Yes**. This allows outbound workgroup calls from the Lync server to be forwarded to the PSTN gateway.
- Leave the *SIP Source Port* set to **5060**.
- Set the *SIP Destination Port* to match the Lync Mediation Server's TCP Listening port (port 5068 by default).

3 Add a similar entry for each mediation server and front-end server in your environment.

4 For multiple mediation server deployment, create one Dialing Table entry for each mediation server.

5 If you are using a hardware load balancer, then create a Dialing Table entry for the balancer.

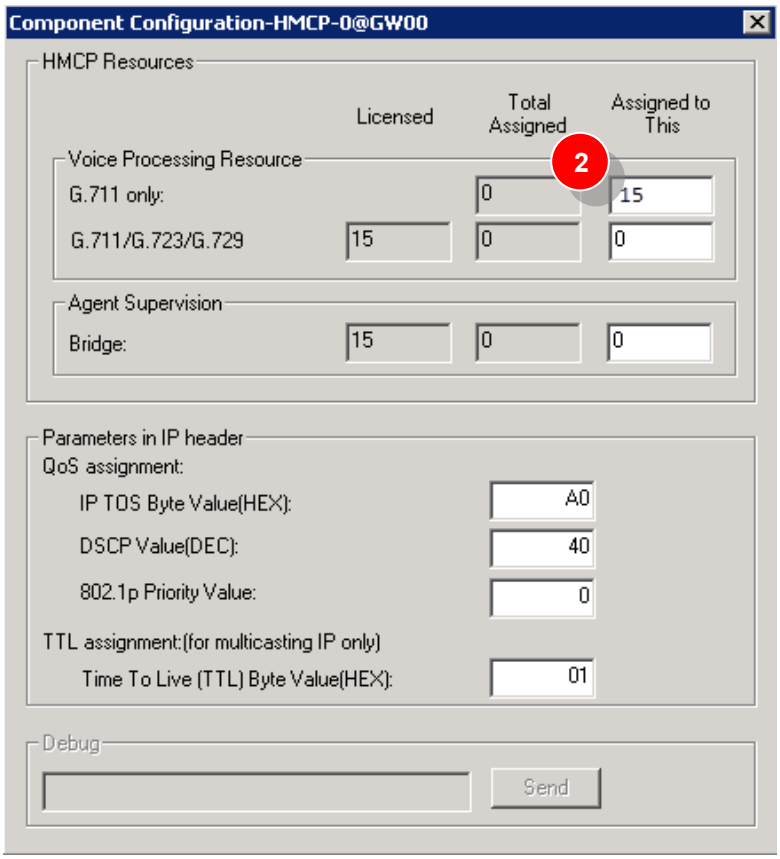
Assign HMCP Resources

To facilitate the voice path between Lync and MaxACD, codec resources must be assigned to the HMCP (Host Media Control Process) component in MaxACD. Each resource represents a single bi-directional audio connection that can be made between the MaxACD, and another VoIP capable device such as Lync, or a SIP media gateway.

By default, no codec resources are assigned to the HMCP component.

1 Double-click **HMCP** in MaxACD Administrator's *Component* view window, and then click **Component Configuration**.

2 Enter the desired number of codec resources (refer to your notes from running the HMCP certification tool) and click **Apply**. A warning will indicate that increasing the number of codec resources may temporarily affect system performance. For this reason, these changes are best made at a time of lowest system usage, such as after hours.



In the figure, fifteen G.711 resources are added.

If you need to change these IP addresses in the future, follow these steps:

1. In Windows, choose **Start** > **All programs** > **AltiGen Lync Server Proxy** > **AltiGen Lync Server Proxy** Configuration.
2. In this tool, you can add a new IP address, edit an existing address, or remove an address as needed. You can also change the Lync Front-end Server Pool or Lync Server Registrar information. After you make your changes, click **Apply**.

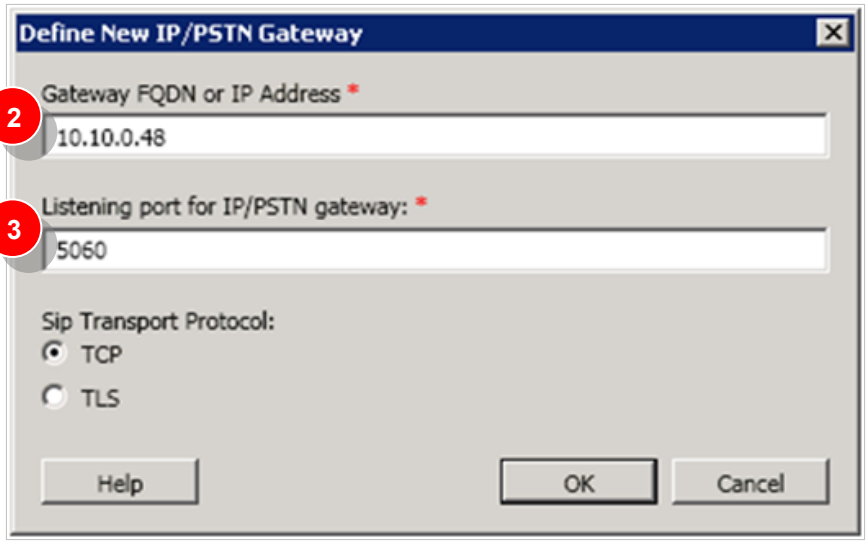
Step 11: Publish the Topology

To add MaxACD as a PSTN Gateway,

1 In Topology Builder, right click **PSTN Gateway** and select **New IP/PSTN Gateway**.

2 Enter the IP address of MaxACD server.

Note: If an FQDN must be used, create a new FQDN in DNS which points to the MaxACD IP address.



Note: In Lync 2013, the dialog box looks different from the above image, which shows the Lync 2010 dialog box.

3 Set the listening port as 5060 and select *TCP* as the SIP transport protocol.

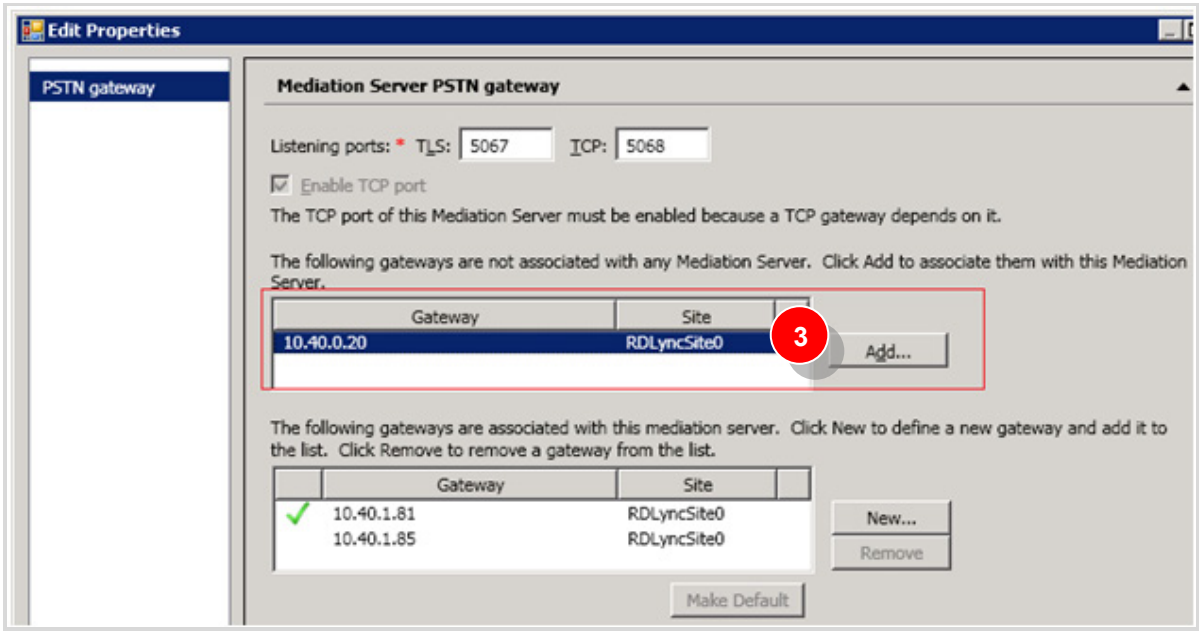
To associate the gateway with Lync Mediation pools,

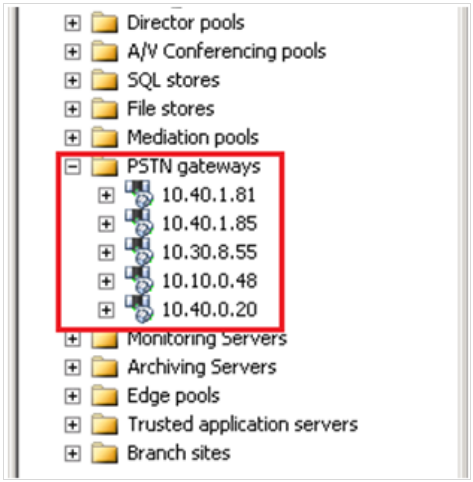
1 In Lync Topology Builder, choose a Mediation pool and open the Edit Properties window.

2 Add the MaxACD-relevant PSTN gateways to the list of "associated with this mediation server."

3 In the example below, highlight gateway 10.40.0.20, which is not associated with any Mediation Server, and click **Add** to associate it with the mediation server, and add the address to that list.

4 Check the **Enable TCP port** checkbox and note that the default TCP listening port is 5068. This port was configured in the IP Dialing Table earlier in this document.


Edit Properties
PSTN gateway
Mediation Server PSTN gateway
Listening ports: * TLS: 5067 TCP: 5068
Enable TCP port
The TCP port of this Mediation Server must be enabled because a TCP gateway depends on it.
The following gateways are not associated with any Mediation Server. Click Add to associate them with this Mediation Server.
Gateway
Site
10.40.0.20
RDLyncSite0
3
Add...
The following gateways are associated with this mediation server. Click New to define a new gateway and add it to the list. Click Remove to remove a gateway from the list.
Gateway
Site
10.40.1.81
RDLyncSite0
10.40.1.85
RDLyncSite0
New...
Remove
Make Default



5 Publish the PSTN gateways listed in the Topology Builder. Right click a PSTN Gateway, and then select **Topology** > **Publish**.

Configuration

This section describes steps you should perform after you have finished installing the product.

Step 12: Configure Firewall/NAT Ports

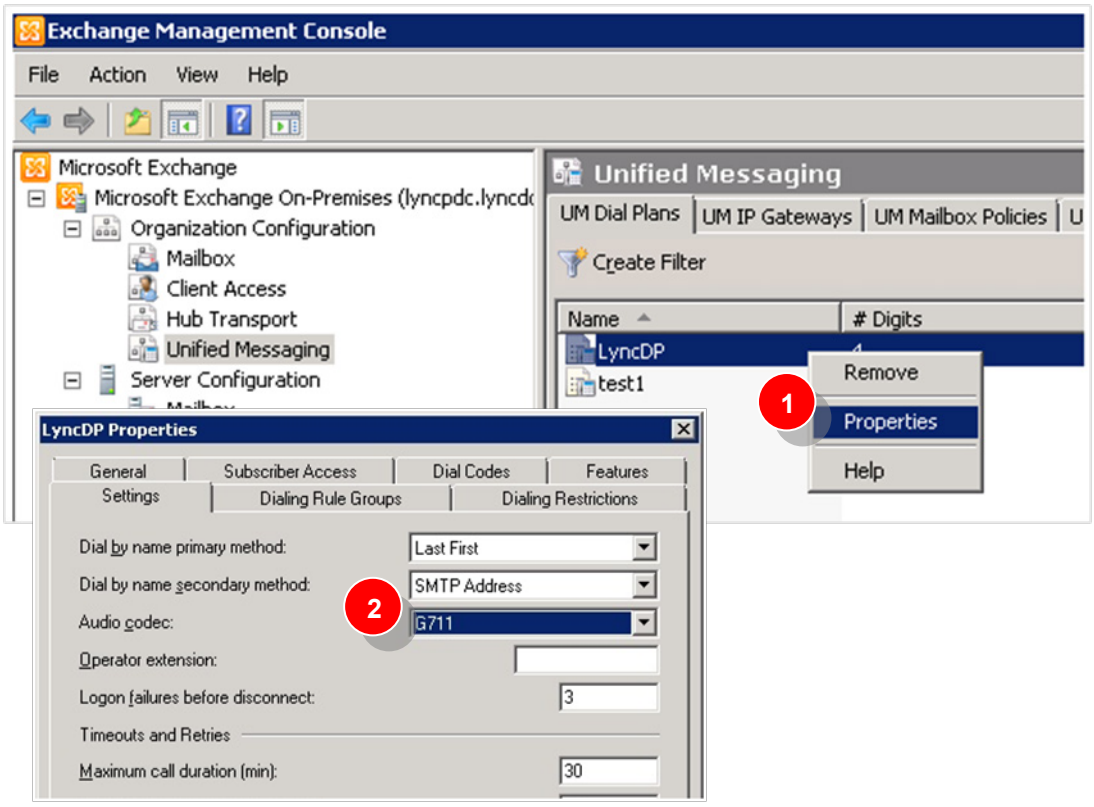
For remote client access, the following firewall/NAT ports must be open and forwarded:

- MaxAgent: TCP ports 10025, 10026, 10028
- MaxSupervisor: TCP 10025, 10027, 10028, 10029, 10050
- Client Applications Auto Update: TCP 10050
- CDR Search: TCP 10025
- Remote Administrator: TCP 10068

Step 13: Configure Exchange Server

Perform the following steps within the Exchange Management console.

1 Under the Unified Messaging Dial Plan, right-click the configured UM Dial Plan and select **Properties**.



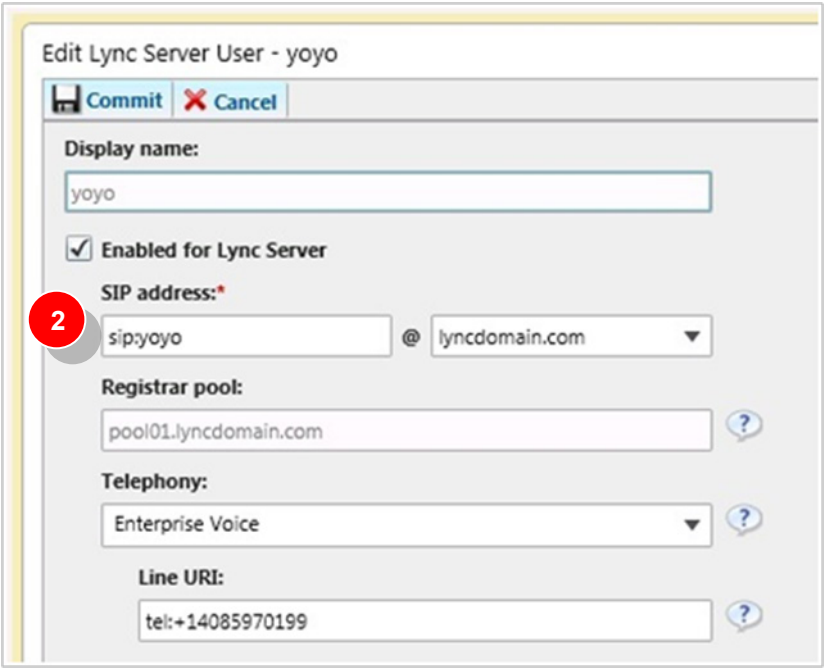
2 Set *Audio codec* to **G711** in the *Settings* tab.

If you want to have workgroup voicemail (or any AltiGen voicemail) synchronized with Exchange, then you must complete additional steps. See Chapter 22 in the *MaxACD Administration Manual* for instructions.

Step 14: Configure a Lync User as a MaxACD Agent Extension

1 Open Lync Server. Under the Lync Server Control Panel, click **User** > **Edit**.

2 Configure the SIP address and Line URI.



3 In MaxACD Administrator, add an agent extension: click **General** > **Extension Configuration** and click **Add** on the bottom left corner.

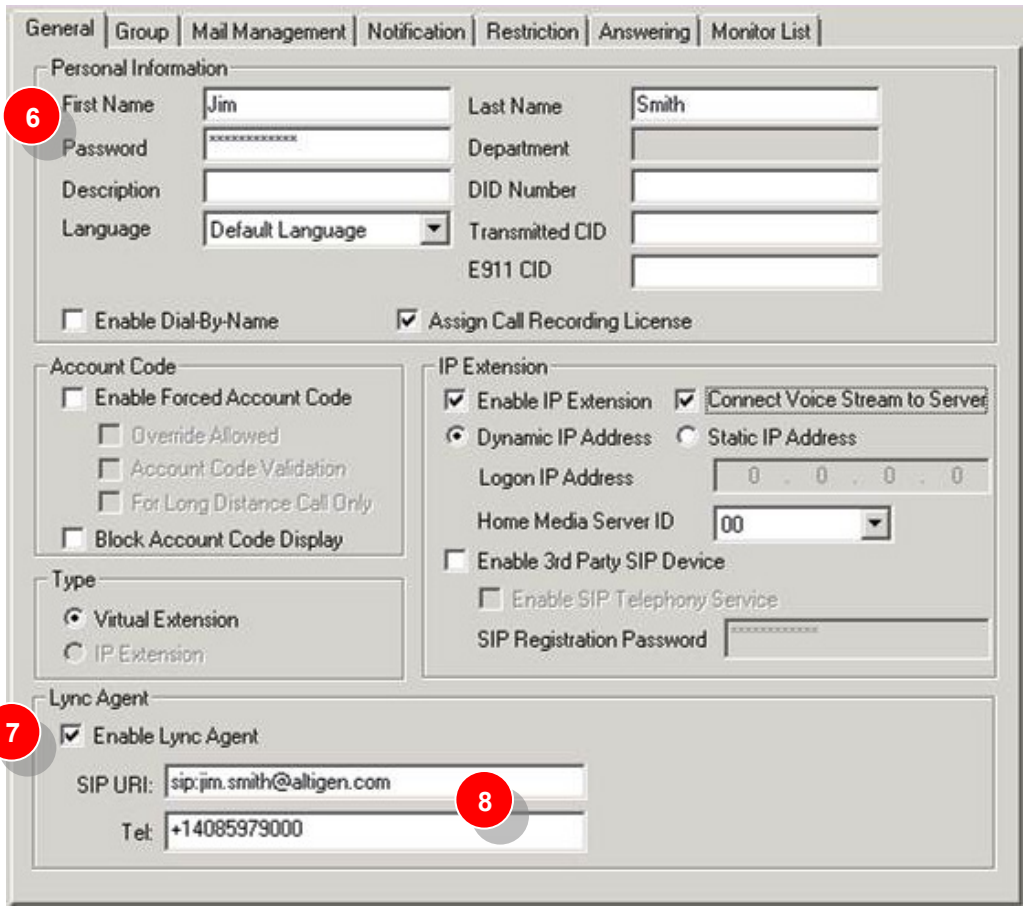
4 Enter the extension number you want to add for a Lync user, and then select **Virtual** for the extension type. Click **OK**.

5 In the Extension Configuration screen, on the left, select the extension number you just added.

6 Enter the name and password.

7 Select the check box *Enable Lync Agent*.

8 Enter both the **SIP URI** and **Tel:** fields from the Lync user configuration. E.164 number format is recommended for the **Tel:** field.


General
Group
Mail Management
Notification
Restriction
Answering
Monitor List
Personal Information
6
First Name
Jim
Last Name
Smith
Password
Department
Description
DID Number
Language
Default Language
Transmitted CID
E911 CID
Enable Dial-By-Name
Assign Call Recording License
Account Code
Enable Forced Account Code
Override Allowed
Account Code Validation
For Long Distance Call Only
Block Account Code Display
IP Extension
Enable IP Extension
Connect Voice Stream to Server
Dynamic IP Address
Static IP Address
Logon IP Address
Home Media Server ID
00
Enable 3rd Party SIP Device
Enable SIP Telephony Service
SIP Registration Password
Type
Virtual Extension
IP Extension
Lync Agent
7
Enable Lync Agent
SIP URI:
sip:jim.smith@altigen.com
8
Tel:
+14085979000

Step 15: Configure Call Routing from Lync Server to MaxACD

Determine targets in MaxACD that should be available to all Lync Users

Although not all Lync users will be MaxACD agents, Lync users may still want to be able to place calls to the MaxACD workgroups, or transfer calls into these workgroups. For this reason, it is recommended that these workgroups be added to the Lync Global Dial Plan.

In this example, workgroups 500-509 are MaxACD workgroups that all Lync users should be able to call.

Create a Normalization Rule that Performs No Translation

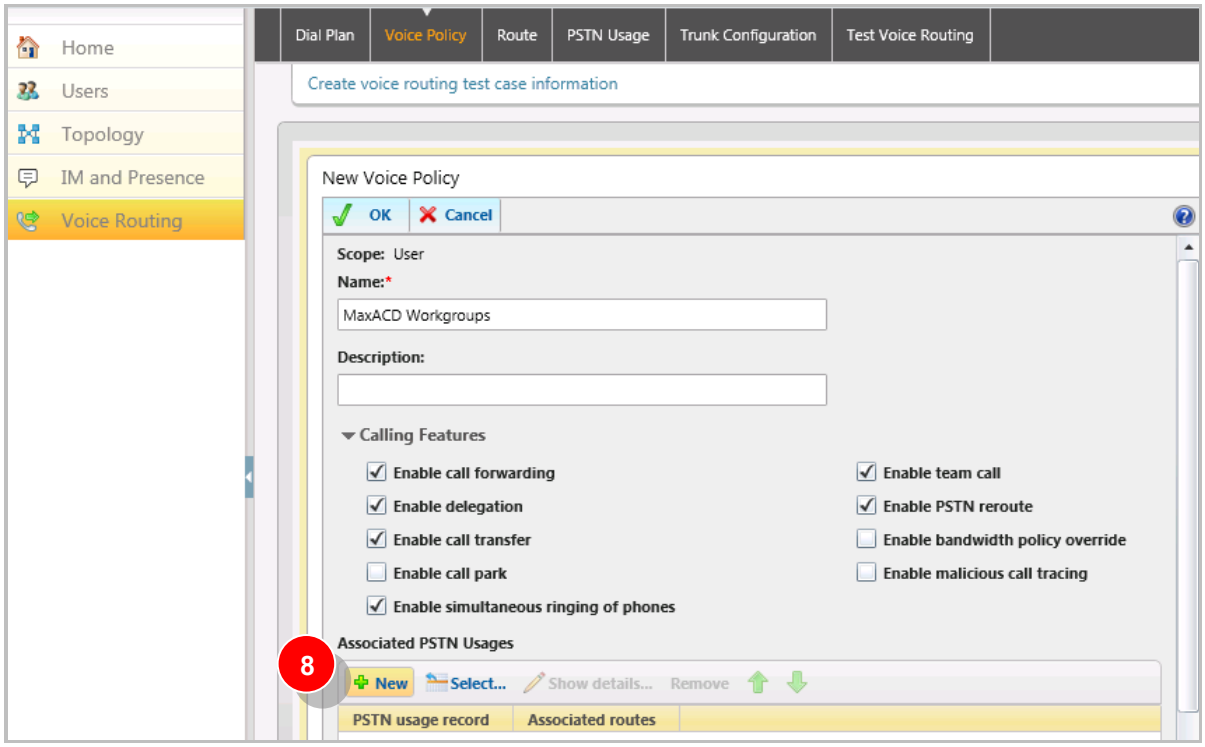
Under **Lync Server Control Panel** > **Voice Routing** > **Dial Plan**, create a new entry that performs no translation for these workgroup numbers:

1. Double click the **Global** dial plan to begin editing.
2. Select **New** under normalization rules to add the new rule. Name this rule "MaxACD Workgroup Normalization."
3. Create a rule that begins with "50" and is exactly 3 digits long.
4. Remove 0 digits from this rule, and add no digits to this rule.
5. Because of this rule, any numbers between 500 and 509 will be normalized exactly as dialed.
6. Create a similar rule for the MaxACD Dial tone (e.g. 222), so that a pattern beginning with 222 that is exactly 3 digits long will have no digit translation performed on it.
7. **Commit** these changes to the dial plan.

Create a Route for These Numbers to the MaxACD Server

Under **Lync Server Control Panel** > **Voice Routing** > **Route**, create a new route:

1. Click **New** to create a new Voice Route. Name this route "MaxACD Workgroups."
2. Click **Edit** and use the following pattern to match for workgroups 500-509: **^(50\d)$**
3. Scroll down the Route page and click on Add… next to *Associated Trunks*.
4. Add the gateway record that corresponds to the MaxACD server.
5. Click OK to return to the Route configuration window.
6. Create a similar Route entry for the MaxACD Dial Tone Pilot Number. Pattern match: *^(222)$*
7. Under **Server Control Panel** > **Voice Routing** > **Voice Policy**, create a new PSTN Usage Record that associates with the Route(s) that you just created.



8 Select **New** under the *Voice Policy* section, and create a PSTN usage record for MaxACD targets. Name this record "MaxACD Workgroup Policy."

9 Click **Select…** in the *Associated Routes* section, and add the routes that were created in the steps above.

10 Click **OK** to return to the Global Voice Policy record, and click **OK** again to return to the **Voice Policy** menu.

11 **Commit** these changes.

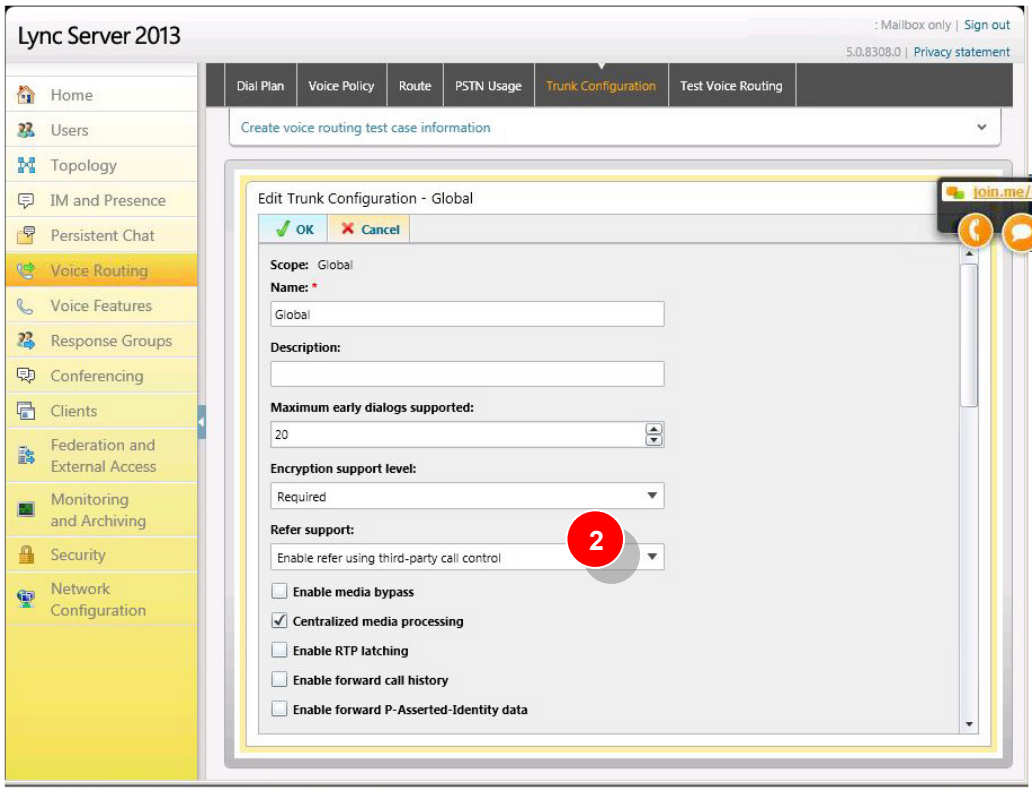
All users assigned to the Global Dial Plan, and Global Voice Policy, should now be able to place calls to MaxACD workgroups.

Enable Third-Party Call Control

Next, enable refer support. The option varies from Lync 2010 to Lync 2013.

1. In the **Lync Server Control Panel**, select **Voice Routing** > **Trunk Configuration**.
2. In Lync 2013, for *Refer support*, select **Enable refer using third-party call control**. This specifies that the third-party control protocol can be used to allow transferred calls to bypass the hosted site.

   In Lync 2010, select the checkbox **Enable refer support**.



3. Click **OK**. Return to the Voice Policy menu and click **Commit** to save these changes.

Step 16: Configure Outbound Workgroup Call Rules

In an outbound call center, the workgroup agent should be able to place 'workgroup' calls so that those call details will be logged to the workgroup for call accounting purposes. Additionally, call recording will be controlled by workgroup settings, and supervisors may be able to barge/coach/monitor these calls.

In order to allow for this, all of the agent's outbound calls MUST route through the MaxACD server. If an agent is ever to participate in any outbound workgroup calling, then ALL of that Lync agent's calls must follow this route.

Make a User Voice Policy for Lync Users Who Will Make Outbound Workgroup Calls

In order to apply the new rules to ONLY Lync users that will utilize features of outbound calling, a new User Voice Policy must be created:

1. Under **Server Control Panel** > **Voice Routing** > **Voice Policy**, select **New** > **User policy**.
2. Name this policy "MaxACD Agent Policy" to indicate that it will apply to MaxACD agents for outbound workgroup calling.
3. Select **New** under *Associated PSTN Usages* to create the PSTN Usage Record to be used by this policy.
4. Name this PSTN Usage Record "MaxACD Agent Usage."
5. Click **New** in the *Associated Routes* section, to create a new route to be used by this policy.
6. Because all calls in this policy will route to the MaxACD server, only a catch-all route is needed. Name this new Route, "Route All to MaxACD".
7. The wild-card pattern to match (.*) can be left as is.
8. In the *Associated Trunks* section, click **Add**…, and associate the PSTN Gateway record for the MaxACD server.
9. Click **OK** to return to the PSTN Usage rule, then **OK** again to return to the Voice Policy configuration, and **OK** once more to return to the general Voice Policy window.
10. Commit the new Voice Policy rules.

Configure Trunks for PSTN calls that Route Through MaxACD server

Outbound calls that will route *through* the MaxACD server must have the leading digit translated in order to access trunks through MaxACD's route access table (typically set to 9 on the MaxACD server). Because the outbound numbers are currently in e.164 format, they will all have a leading "+" (plus) symbol. A new Pool Trunk rule will be used to change the leading + to a 9 as follows:

1. Under **Server Control Panel** > **Voice Routing** > **Trunk Configuration**, click **New** > **Pool trunk**.
2. Chose the PSTN Record for the MaxACD server.
3. Under *Associated Translation Rules*, click **New** to create a new translation rule.
4. Name this rule "Replace + with 9".
5. Use "9" as the Digits to add. Keep all other settings at default.
6. Click **OK** to save this rule, Click **OK** again to return to the main Trunk Configuration window.
7. Commit the new Pool trunk configuration.

Assign the New Voice Policy to Lync Users Who Make Outbound Workgroup Calls

Only Lync users that are assigned to this new voice policy will have their outbound calls route *through* the MaxACD server. Note that these Lync users must also be configured as MaxACD agents as well in order to get any of the benefits of outbound workgroup calling. In order to assign this policy to the Lync users, do the following:

1. Go to **Server Control Panel** > **Users**, and search for the user(s) that need to have this policy applied to.
2. Double-click the user to edit the user's configuration.
3. Change the user's assigned Voice Policy to "MaxACD Agent Policy" (The policy name assigned in step 2 of the section titled "**Create a new User Voice Policy for Lync users that will participate in Outbound Workgroup calling**" of this document.
4. Click **Commit** to save these changes.

Because of the steps above, if this user dials 1-888-258-4436, the Dial Plan should normalize the number to +18882584436. The Voice Policy will be used to select the "Route All to MaxACD" route, directing the call to the MaxACD server. The Trunk Configuration will then change the number sent to MaxACD from **+**18882584439 to **9**18882584436.

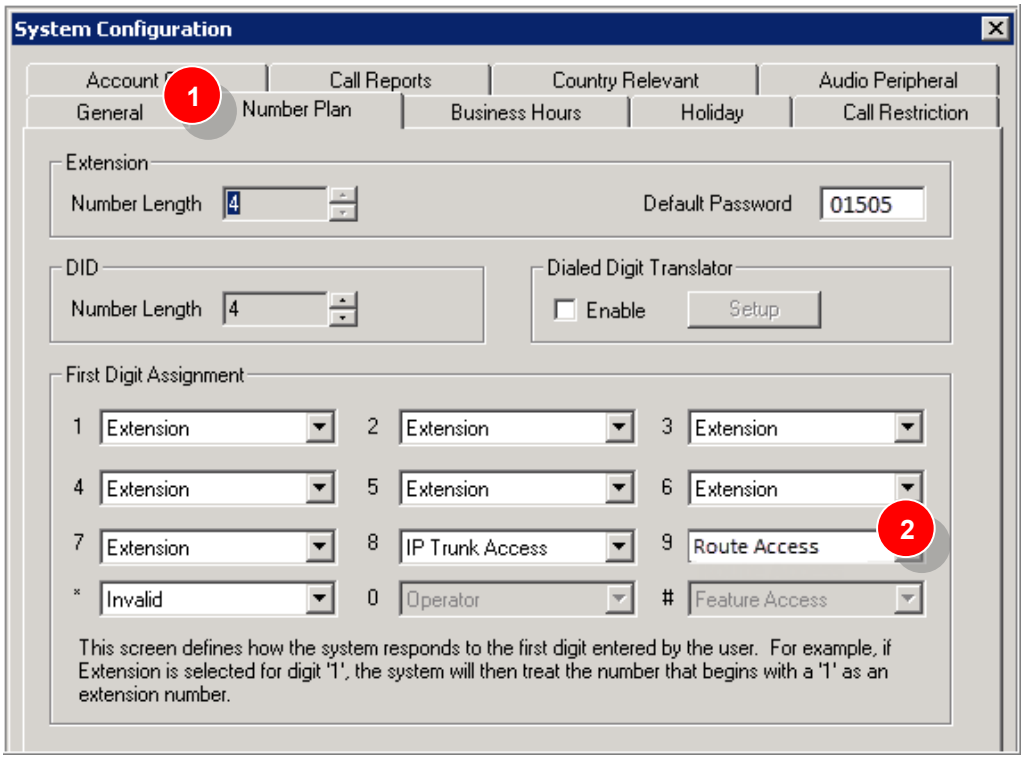
The next section provides instructions for routing through MaxACD to the gateway.

Step 17: Configure MaxACD for Lync Routing

Configure the Number Plan to include a route access code for PSTN calls and setup Out Call Routing.

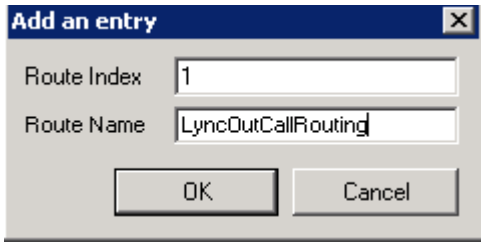
1 In MaxACD Administrator click **System**, and then click the **System Configuration** > **Number Plan** tab.

2 Under *First Digit Assignment*, assign an unused number to *Route Access*. Number 9 is used in the next example. Assign another unused number to **IP Trunk Access**. Number 8 is used in the example.



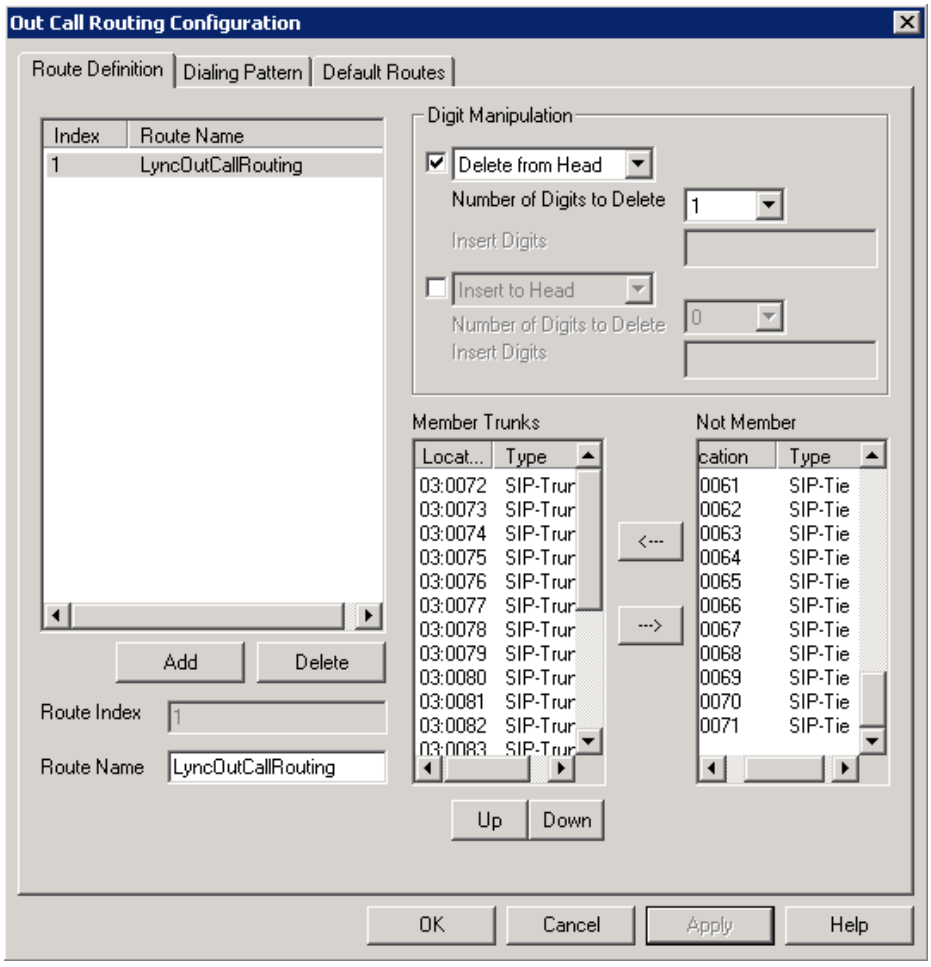
Note: An IP Trunk access digit should be assigned; this digit should be applied to all SIP tie trunks.

3 Under **General** > **Out Call Routing Configuration**, on the *Route Definition* tab, click **Add**.



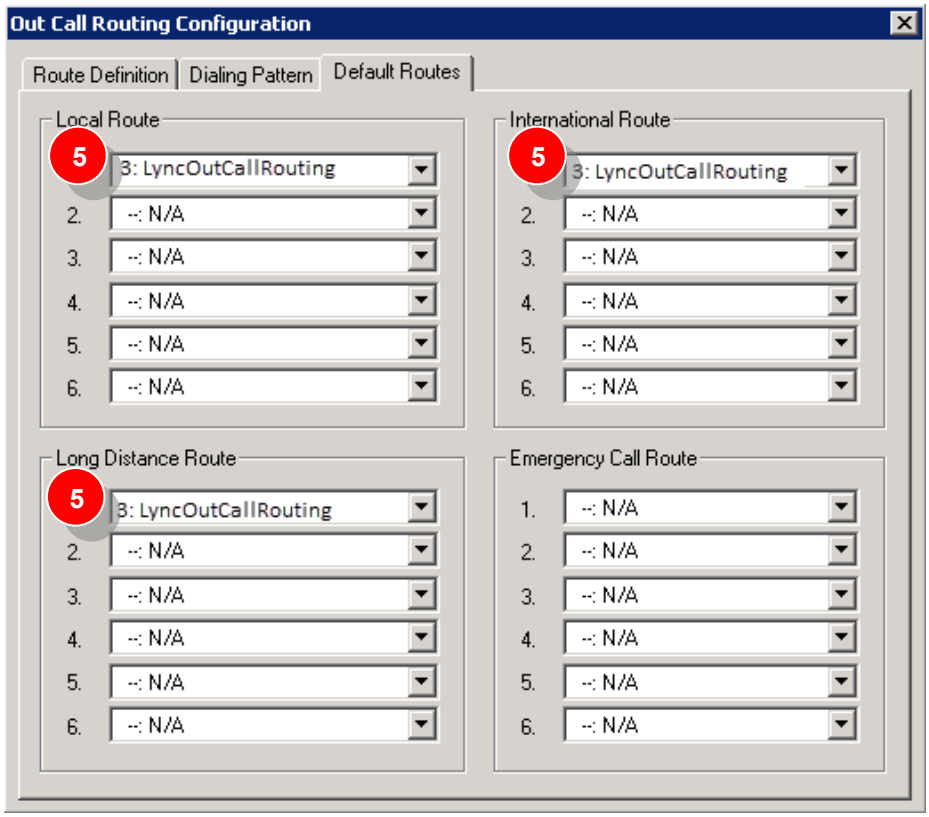
4 Add an outcall routing entry and click **OK**.

5 Select SIP trunks for outbound calls by adding trunk channels to Member Trunks. Then click **Apply** to save the changes.



6 Click the **Default Routes** tab.

7 Select the Route Definition you just added under the "Local Route, "Long Distance Route," and "International Route" sections. Click **OK** to save the changes.


Out Call Routing Configuration
Route Definition
Dialing Pattern
Default Routes
Local Route
5
3: LyncOutCallRouting
2. --: N/A
3. --: N/A
4. --: N/A
5. --: N/A
6. --: N/A
International Route
5
3: LyncOutCallRouting
2. --: N/A
3. --: N/A
4. --: N/A
5. --: N/A
6. --: N/A
Long Distance Route
5
3: LyncOutCallRouting
2. --: N/A
3. --: N/A
4. --: N/A
5. --: N/A
6. --: N/A
Emergency Call Route
1. --: N/A
2. --: N/A
3. --: N/A
4. --: N/A
5. --: N/A
6. --: N/A

Step 18: Configure Voicemail Access

Now you will make Lync Agent's personal voice mail accessible through MaxAgent for Lync.

1. In MaxACD Administrator, click **System** > **Voice Mail Configuration**.
2. Select **Synchronize with Exchange**.

With the same Exchange Synchronization setting, workgroup voicemails are synchronized back to Exchange Server so that voice messages can be retrieved from workgroup email accounts.

Refer to Chapter 22 in the *MaxACD Administration Manual* for detailed Exchange Integration configuration instructions.

Troubleshooting

This section provides some tips for troubleshooting various issues with MaxACD.

- For MaxACD issues, in addition to gathering a complete set of traces, please provide all log files in this folder on the Lync Front-end server:

  C:\AltiLyncServProxy\Log

- For MaxAgent issues, provide traces from the client log files from this folder:

  C:\Users\<user>\Application Data\AltiGen\MaxAgent For Lync\Logfiles\ApplicationLog.log

- For reproducible connection or routing issue, please provide Wireshark (www.wireshark.org) packet capture from the MaxACD system and possibly the Lync Server trace.

- If the issue is related to a call transfer, make sure that the *Enable refer support* option in Lync Trunk Configuration is enabled. MaxACD needs a referral from the Lync server to finish transferring calls.

  To check this option, log into Lync Server and choose **Voice Routing** > **Trunk Configuration**. Double-click **Global** to see that option.

For further tips, log into the AltiGen Partner Knowledgebase (http://thinklync.altigen.com) and search for the article, "MaxACD Troubleshooting." This article contains a list of common problem areas and configuration settings that you should check before you contact AltiGen Support. It also explains how to run traces and gather MaxAgent logs.

Performance

The following table illustrates feature capabilities based upon the type and speed of your processor, the amount of memory available, and the size of the hard drive.

Performance: MaxACD 6.5 for Lync		
System Configuration (Windows 2008 R2 SP1)	**Vmware All-in-one**	**Installed on 2008 Telecom Server All-in-one**
Virtualization software version	Vmware version (7)	
CPU	Intel Xeon E5620 2.4GHZ	Intel Core2 6600 2.4G HZ
Memory	4G	2G
Hard Drive	50G Allocated	150G
Maximum HMCP Resources		
Max G.711 Voice Processing Resources	600	600
Max G.723/G.729 Processing Resources	60	60
Max Recording Sessions	256	256
Max Number of Lync Extensions	512	512
Max Number of Virtual Extensions	2000	2000
Max number SIP Trunks	300	300
Maximum Group/Agent Configuration		
Max Number of Workgroups	128	128
Max Number of Agents Configured per Workgroup	512	512
Max Number of Logon Agents per System	256	256
Max Total Number of Agents Configured in all Workgroups	640	640
Maximum CT Sessions		
Max Number of MaxAgent Sessions	256	256
Max Number of MaxSupervisor Sessions	20	20
Max Number of Agent Appearances in MaxSupervisor	512	512
Max Number of Workgroups Monitor in MaxSupervisor	10	10
Max Number of MaxAdmin Sessions	5	5
Maximum Call Volume		
Max Hourly Call Volume	5000	5000